# UNIVERSIDAD POLITÉCNICA SALESIANA
# SEDE QUITO

**CARRERA: INGENIERÍA DE SISTEMAS**

**Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS**

**TEMA:**

**ANÁLISIS Y DISEÑO DE MEDIDAS PREVENTIVAS APOYADAS EN LA INFORMÁTICA FORENSE PARA MEJORAR LOS NIVELES DE SEGURIDAD DE LA INFORMACIÓN MANEJADA POR EL SERVICIO DE MESA DE AYUDA PRESTADO POR LA EMPRESA TATA**

**AUTOR:**

**WILLIAM HENRY CHACÓN BONIFAZ**

**DIRECTOR:**

**FRANKLIN EDMUNDO HURTADO LARREA**

**Quito, mayo de 2015**

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE TITULACIÓN**

Yo, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaro que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.
Quito, mayo de 2015.

---

William Henry Chacón Bonifaz
CC: 171884207-1

## DEDICATORIA

A mi Madre, que vive una lucha admirable todos los días y nunca se rinde ante los problemas cotidianos que puedan presentarse, por toda la fuerza brindada, confianza, ánimo y apoyo necesario en el trascurso de mi vida universitaria; siendo mi apoyo incondicional en toda esta etapa, a mi Padre que se encuentra en el cielo que con la bendición de él pude culminar mis estudios, a mi hermano que con su ayuda, consejos diarios culmine mis estudios universitarios.

## AGRADECIMIENTO

A la Universidad Politécnica Salesiana por todas las enseñanzas recibidas, consejos, anécdotas y sobre todo experiencias que se presentó en toda mi vida universitaria y, de una manera muy especial agradezco a quienes fueron guía y apoyo para culminar esta tesis Ing. Franklin Hurtado.

# ÍNDICE

## ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# ÍNDICE DE ANEXOS

## RESUMEN

El trabajo describe el análisis y diseño de medidas preventivas apoyadas en la informática forense para mejorar los niveles de seguridad de la información manejada por el servicio de mesa de ayuda que presta la empresa “TATA” a “TELEFÓNICA” utilizando herramientas (software) y metodologías que nos permita identificar posibles vulnerabilidades en la organización, con el objetivo de diseñar medidas preventivas que permitan mejorar los procesos y la gestión de la información para brindar el soporte TI a los usuarios internos del cliente.

## ABSTRACT

The paper describes the analysis and design of preventive measures supported in computer forensics to improve security levels of information handled by the help desk service provided by the company "TATA" - "TELEFÓNICA" using tools (software) and methodologies that allow us to identify potential vulnerabilities in the organization, with the aim of designing preventive measures to improve processes and information management to provide TI support to internal users of the client.

# INTRODUCCIÓN

El crecimiento de la empresa ha obligado a que sea más competitiva, y busque alternativas tecnológicas, procesos que permitan gestionar la información de sus clientes. Es aquí donde la seguridad de la información e informática es trascendental para garantizar el buen uso de los datos que se manejan en las mismas. Es decir, presentar un escenario donde se garantice la disponibilidad, integridad, confidencialidad de la información y los sistemas de almacenamiento.

En el capítulo uno se describe los conceptos y lineamientos básicos utilizados en el desarrollo del caso de estudio.

En el capítulo dos se describirá la situación actual del Service Desk, la evaluación del entorno informático, y se identificará los posibles problemas del caso de estudio mediante entrevistas, Check List y pruebas de vulnerabilidades mediante software vigentes.

En el capítulo tres se presentará el informe y resultados del caso práctico, con el fin de realizar un diseño de medidas preventivas de seguridad informática.

Al finalizar la investigación se presentan las conclusiones obtenidas y recomendaciones a lo largo del trabajo.

# CAPÍTULO 1
# FUNDAMENTO TEÓRICO

## 1.1. Historia de la informática forense

> La historia de la informática forense es difícil de predecir donde apareció, mediante estudios realizados se puede decir que en los países desarrollados como Estados Unidos, China, Japón, España, empezaron el análisis con la policía, y con el pasar del tiempo se dieron cuenta que los criminales empezaron a tener demasiado conocimiento técnico referente a la informática (Informática forense, 2006).
>
> Las organizaciones pequeñas, medianas, y grandes diseñaban su infraestructura sin tener un plan de seguridad, y mediante la operación aparecen personas que se dedicaban al espionaje y violación de información, causando pérdidas económicas e incluso desaparición de las entidades, mediante estos ataques la policía analiza los casos y realizan investigaciones frecuentes para evitar que una organización se vea afectada en estos acontecimientos (Data Recover Center, 2014).

A través de esto los científicos explotaron esta disciplina para ejercer la informática forense en nuestro medio; sin embargo aún no ha sido debidamente identificada, de tal forma que estimule su estudio e investigación.

Mediante el desarrollo del estudio de informática forense se dio a conocer el tema en todas las organizaciones, haciendo que estas tomarán conciencia en el déficit y problemas que puede causar si no se tiene un plan de seguridad adecuado.

En la actualidad este tema está tomando mucho interés en países avanzados y en nuestro país se ha considerado normativas que fomenten una cultura de seguridad de la información, es decir políticas internas que permitan mejorar la integridad, disponibilidad, confidencialidad.

## 1.2. ¿Qué es la informática forense?

A la informática forense se le puede definir como un estudio de vulnerabilidades o fallas sobre infraestructuras de computación, sistemas informáticos, estructura de una red, con la finalidad de buscar evidencias que colabore a llevar un caso judicial (forense, Informática, 2010).

Mediante este problema la informática forense extraerá, analizará, documentará evidencias que colabore a proponer una solución mediante el uso de hardware y software.

"La informática forense consiste en investigar sistemas de información con el fin de detectar evidencias de vulnerabilidad en los mismos con el fin de perseguir objetivos preventivos u objetivos correctivos" (Ramírez, 2008).

### ¿Para qué sirve?

"Para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información" (Mota, 2013).

## 1.3. ¿Cuál es el objetivo de la informática forense?

- Compensar de los daños causados por los criminales o intrusos.
- Perseguir y procesar judicialmente a los criminales informáticos anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.
- Aplicar medidas como un enfoque preventivo (Giovanni Zuccardi y Juan Gutierrez, 2006).

## 1.4. Importancia de la Informática Forense

La informática Forense hoy en día es de gran utilidad y se desarrolla en función de la necesidad de determinar eventos y tareas probatorias en el caso de un proceso legal y/o para apoyar a la informática para mejorar los procesos de seguridad en una organización.

> Es decir, la importancia de la informática forense tiene un papel como sistema preventivo, sirve para auditar, mediante la práctica de diversas técnicas para probar que los sistemas de seguridad cumplen con puntos prioritarios. Los resultados de las auditorías sirven como objeto para mejorar los niveles de seguridad de las tecnologías de información, así mismo elaborar políticas de seguridad para mejorar el rendimiento (Ramírez, 2008).

## 1.5. Estándares para el análisis Forense.

Para el estudio o análisis de la informática forense no existe un criterio unificado para ejecutar o dar seguimiento a un evento. Es por esto, que la informática forense se ha relacionado con la seguridad informática para fundamentar su trabajo. Es decir, la informática forense ha fundamentado su accionar en estándares y criterios predefinidos en códigos de buenas prácticas.

Como ejemplo se puede considerar los siguientes estándares:

### 1.5.1. CP4DF "Código de prácticas para digital forensics"

Es un documento de criterios que permiten guiar y asegurar actividades concernientes con el análisis de evidencia digital. Provee de recomendaciones y cubre aspectos legales, policiales, operacionales como requerimientos técnicos para adquisición, análisis, reporte de evidencia, colaboración con otros grupos de investigación, gestión de casos; soporte a la fuerza de la ley, desarrollo de políticas de seguridad para respuesta a incidentes y plan preventivo y de continuidad (Roger Carhuatocto, 2008).

"CP4DF no es un manual técnico para análisis de computación forense, CP4DF es un manual basado en criterios siguiendo el asesoramiento de la comunidad y expertos" (Roger Carhuatocto, 2008).

Los criterios definidos en el manual de CP4DF permiten al perito o técnico informático contar con un marco conceptual que permite abordar procesos de investigaciones sobre evidencia digital de acuerdo a los siguientes criterios:

- Asegurar la escena con personal competente que conozca sobre informática forense.

- Identificar las evidencias según prioridades del cliente, dispositivos de almacenamiento de información externa o las leyes del país.

- Preservar la evidencia.

- Analizar las evidencias para conocer el propósito del siniestro y criticidad al cumplimiento del mismo.

- Presentar la información clara, concisa y estructurada mediante un lenguaje no técnico.

"El público al que va dirigido son policías, detectives, abogados, técnicos, auditores, expertos y personas interesadas" (Perícia Forense aplicada a informática, 2003).

### 1.5.2. RFC3227

"El RFC3227 es una guía para recolectar y levantar evidencia, escrita en febrero del 2002, es una guía de alto nivel para recolectar y archivar datos relacionados a intrusiones, también explica algunos conceptos relacionados con la parte legal" (UTN-FICA-EISIC).

Los principios o directrices básicos establecidos en esta guía para la recopilación y almacenamiento de las evidencias, se desarrollan en función de los siguientes aspectos:

- Visualizar y analizar el escenario en el cual se ha producido el hecho y se desea captar las evidencias.

- A la hora de recopilar las evidencias, minimizar los cambios que alteren el escenario y eliminar los agentes externos que puedan hacerlo.

- Si hay dudas en la recolección y el análisis de evidencias se debe dar prioridad a la recolección de evidencias en un siniestro informático. (Lizeth Arely, 2014)

La copia de información debería realizarse a nivel binario para no alterar a ninguno de los datos.

### 1.6. Fases de la informática forense

Las principales fases de la informática forense son:

- **Identificación del incidente**

"Es importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático" (José Manuel Ferro Veiga).

La identificación del incidente hace mención al inicio de la investigación de la informática forense y el de realizar un análisis del problema ocurrido. Se recibe toda la información sobre un incidente que fue ocasionado y siendo verificado el mismo, además se debe establecer que sucedió en el momento del incidente, al momento del acceso a la información, y las pruebas del escenario y sus circunstancias o motivos que pudo ser ocasionado el incidente.

- **Recopilación de evidencias**

En esta fase se recoge todas las pruebas digitales del incidente, la evidencia debe ser suficiente, confiable, relevante y útil para lograr los objetivos de la informática forense.

- **Preservación de la evidencia**

Este es una de las fases más críticas de la metodología, debido a que cuando se haya comprobado el delito informático de la empresa u organización, se debe llevar un proceso de manera judicial; este proceso se debe realizar de manera inmediata con las respectivas pruebas.

Hay que tener en cuenta que siempre hay que evitar los cambios que pueden ocurrir en las evidencias y si no se logra se necesita registrarlo, documentarlo y

justificarlo, siempre que sea posible con testigos que puedan corroborar las acciones (Arturo Palacios Ugalde, 2010).

- **Análisis de la evidencia**

En el análisis de la evidencia involucra todas las tareas con sus objetivos orientados a localizar y extraer evidencias digitales relevantes para la investigación, el análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo, y hay que asegurarse que la persona que esté realizando el análisis de la evidencia se encuentre totalmente capacitado para ello.

- **Documentación y presentación de los resultados**

Conociendo todas las etapas anteriores, consiste en realizar la elaboración de la documentación basada en los resultados obtenidos en las etapas anteriores, con el propósito de proporcionar al lector toda la información. La presentación de los resultados debe ser de forma clara y concisa que sea entendible para las personas y tener una discusión clara del tema.

El análisis de pruebas que permitan determinar el grado de incidencia de los problemas citados en la empresa de estudio servirá como instrumento básico para comprender los problemas que pueden ocurrir en una empresa que brinda servicios de Outsourcing, y así entender porque las organizaciones que brindan servicios TI deben realizar controles periódicamente con la finalidad de determinar sus seguridades tanto físicas como lógicas.

Fases de la informática forense

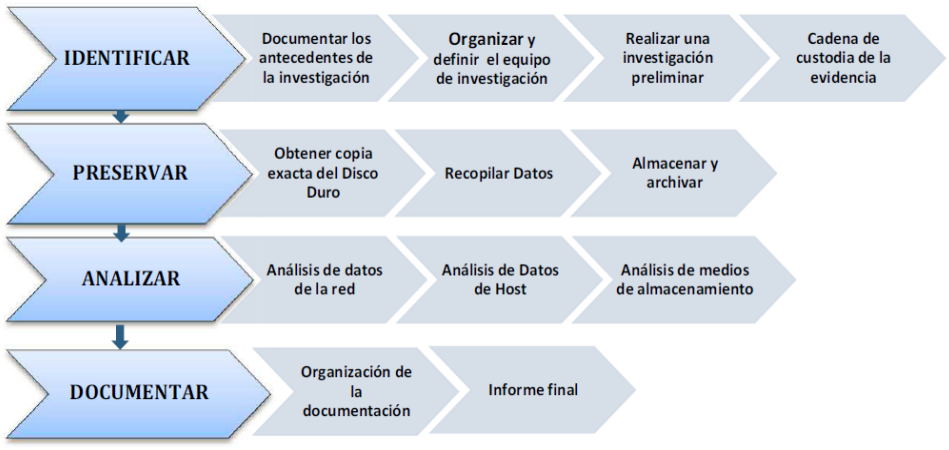



*Figura 1*. Fases de la informática forense.
Fuente: (Elizabeth, Jácome Ortega Alexandra, 2011)
Elaborado por: (Elizabeth, Jácome Ortega Alexandra, 2011)

### 1.7. Seguridad de información

El término de seguridad de información significa evitar la pérdida de la información y protegerla de los distintos accesos a los sistemas de información, es decir mantener un control del uso, divulgar a terceras personas, alterar o modificar, acceso no autorizado o su destrucción de la información prioritaria de una empresa.

Hoy en día la información es el activo principal de toda organización. Es por esto, que toda empresa busca alternativas que permitan tomar medidas preventivas y reactivas que permiten salvaguardar la información; con el fin de mantener confidencialidad, disponibilidad e integridad de los datos.

> Mediante el análisis de expertos en seguridad informática, más del 70% de las violaciones e intrusiones se realiza por el personal interno de una organización, debido a que conocen los procesos, metodologías, y tienen acceso a la información confidencial de la empresa y el cliente, es decir los datos extraídos puede causar una mala imagen en el mercado y el mal funcionamiento de la organización. (Revista Red, 2002)

Muchas veces las personas asocian el tema de seguridad únicamente al manejo o uso de páginas web, sin meditar acerca del universo que abarca la seguridad. Es así, que en el medio existen pocos profesionales formados académicamente y con la experiencia en esta área. Por este motivo, la mayoría de los técnicos que han incursionado en el tema de seguridad han desarrollado sus destrezas en la experiencia de sucesos ocurridos en sus labores diarias y publicaciones de problemas de seguridad; limitando estos conocimientos, en la mayoría de los casos al uso de parches de sistemas operativos, antivirus, antispyware, firewall y en algunos casos seguridad en redes, sin considerar que ésta abarca muchos ámbitos más.

> Es común, pensar que las empresas se encuentran protegidas y preparadas para evitar o minimizar un ataque o riesgo informático y se confían en que nunca ocurrirá alguna amenaza que afecte la seguridad de la empresa, sin pensar que las amenazas y vulnerabilidades son cambiantes en el tiempo, ya que existen personas que se encuentran en continua preparación y actualización para transgredir sistemas con el propósito de apropiarse de la información con fines no éticos (MacAfee, 2013).

Mediante lo expuesto anteriormente se definen algunos marcos de referencia que nos permiten realizar un análisis de la situación actual del Service Desk, como el grado de madurez y seguridad en función a: red, instalaciones, personal, procedimientos.

## 1.8. Marcos de referencia para la revisión y evaluación de la situación actual del Service Desk

Dentro de los marcos de referencia reconocidos a nivel mundial para la evaluación del estado actual de TI, se encuentran COBIT 4.1, ISO 27002 e ITIL.

Cada uno de estos marcos tienen definidos controles para la seguridad de la información y el manejo de una área de TI, su revisión está orientada a mejoras en el servicio, en el proceso y el trato que la empresa debe tener para con su personal. A lo largo de los tiempos cada marco de referencia ha tomado su orientación siendo de tal manera clasificada por la orientación del cumplimiento de sus controles de revisión.

COBIT ha sido definido o utilizado en su mayoría para revisión de procesos de TI y su mejora en los controles de una sistema de gestión de gobierno TI, los estándares ISO tienen varias ramas definidas para el análisis, la gama de la ISO 27000 en adelante han sido tomadas para la revisión de seguridades en la información e instalaciones, por su parte ITIL está orientada a la mejora de servicios incluido el personal que presta el servicio, por lo tanto a continuación se detallará cada una de los marcos de referencia utilizados en el desarrollo de la presente tesis para el análisis del estado actual del proyecto Service Desk TCS- Telefónica.

### 1.8.1. COBIT 4.1

"COBIT es un acrónimo para Control Objectives for Information and related Technology (Objetivos de Control para tecnología de la información y relacionada); desarrollada por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI)" (IT Governance Institute, 2007).

COBIT es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas implican.

"La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TI, incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez" (IT Governance Institute, 2007).

"Permite a las empresas aumentar su valor TI y reducir los riesgos asociados a proyectos tecnológicos. Ello a partir de parámetros generalmente aplicables y aceptados para mejorar las prácticas de planeación, control y seguridad de las Tecnologías de Información" (Transforma Consultoría, 2012).

COBIT contribuye a reducir las brechas existentes entre los objetivos de negocio, y los beneficios, riesgos, necesidades de control y aspectos técnicos propios de un proyecto TI, proporcionando un marco referencial lógico para su dirección efectiva (IT Governance Institute, 2007).

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas (IT Governance Institute, 2007).

Principios de COBIT

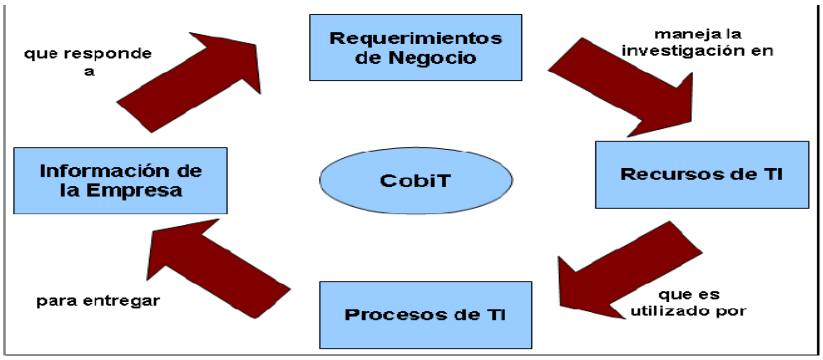



*Figura 2.* Principios básicos de COBIT
Fuente: (IT Governance Institute, 2007)
Elaborado por: (IT Governance Institute, 2007)

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear (IT Governance Institute, 2007).

- Planear y Organizar (PO): proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).

- Adquirir e Implementar (AI): proporciona las soluciones y las pasa para convertirlas en servicios.

- Entregar y Dar Soporte (DS): recibe las soluciones y las hace utilizables por los usuarios finales.

- Monitorear y Evaluar (ME): monitorear todos los procesos para asegurar que se sigue la dirección provista (IT Governance Institute, 2007).

Recursos de TI

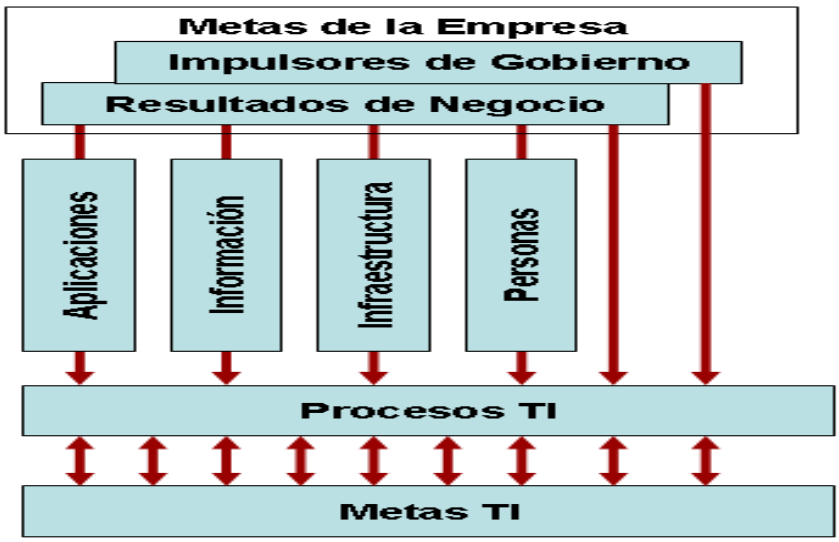



*Figura 3.* Gestión de los recursos de TI para entregar metas de TI
Fuente: (IT Governance Institute, 2007)
Elaborado por: (IT Governance Institute, 2007)

Los procesos requieren controles, control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Representación gráfica de los modelos de madurez

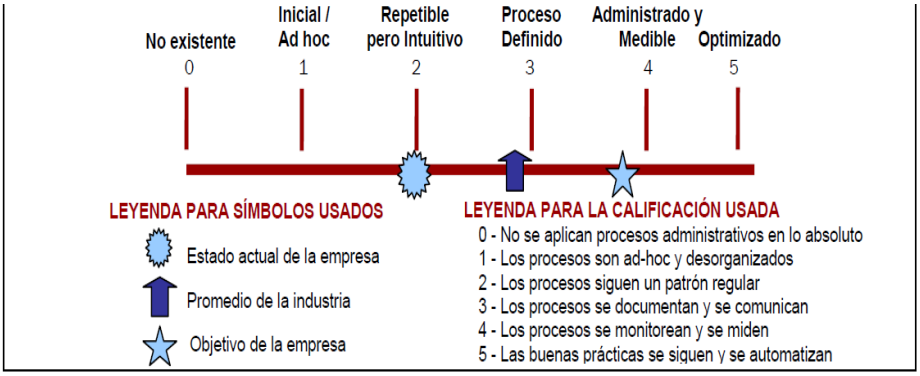



*Figura 4.* Modelo de madurez de COBIT
Fuente: (IT Governance Institute, 2007)
Elaborado por: (IT Governance Institute, 2007)

COBIT es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control, para lo cual ha definido una calificación a la madurez de la empresa según sus procesos y controles. El tema de procesos de TI es esencialmente complejo y subjetivo, por lo tanto, es más fácil abordarlo por medio de evaluaciones fáciles que aumenten la conciencia, mediante observación directa y encuestas al personal que los ejecuta dentro de la empresa, permitiendo que logren un consenso amplio y que motiven la mejora de los mismos en función de la madurez de la empresa. Estas evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor proceso por proceso y al final determinar un promedio para toda la organización. De cualquier manera, se requiere experiencia en el proceso de la empresa que se está revisando es decir se debe conocer el negocio principal de la organización.

La ventaja de un modelo de madurez que ofrece COBIT es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

Modelo genérico de madurez

**Figura 13 – Modelo Genérico de Madurez**

**0 No Existente**- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

**1 Inicial**- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

**2 Repetible**- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

**3 Definido**- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

**4 Administrado**- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

**5 Optimizado**- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

*Figura 5.* Modelo genérico de madurez de COBIT
Fuente: (IT Governance Institute, 2007)
Elaborado por: (IT Governance Institute, 2007)

### 1.8.2. ISO 27002

Es creada particularmente para tener una adecuada seguridad siguiendo una guía de buenas prácticas que ayuda a las organizaciones implementar, mantener y mejorar su gestión de seguridad de información. (Bormart, 2009-2012)

La definición de la norma ISO 27002 es preservar la confidencialidad teniendo en cuenta que solo las personas autorizadas pueden tener acceso a la información con diferentes niveles de acceso, preservar la integridad para asegurar que la información sea exacta y completa que no sea manipulada y por último preservar la disponibilidad asegurando que los usuarios autorizados tengan acceso a la información.

> Es por eso que la información es un activo importante en toda organización por lo tanto necesita cumplir con ciertos parámetros para reducir el riesgo, amenazas y vulnerabilidades, esto nos permitirá asegurar la continuidad del servicio y maximizar las oportunidades de negocio. (Icontec, 2007)

En este contexto si se produce una incidencia, los daños se minimizan y se produce un ahorro de costos debido a una racionalización de los recursos.

La norma ISO 27002 contiene 39 objetivos de control y 133 controles las cuales están agrupadas en 11 dominios, la siguiente tabla muestra cada uno de los dominios de la norma:

Tabla 1. *Marco Normativo ISO 27002*

| **Marco Normativo ISO 27002** |
|---|
| 1, Política de Seguridad |
| 2, Organización de seguridad |
| 3, Clasificación y control de activos |
| 4, Aspectos humanos de la seguridad |
| 5, Seguridad física y ambiental |
| 6, Gestión de comunicaciones y operaciones |
| 7, Sistema de control de accesos |
| 8, Desarrollo y mantenimiento de sistemas |
| 9, Gestión de incidentes de seguridad |
| 10, Plan de continuidad del negocio |
| 11, Cumplimiento |

Nota. (NimboSystem, 2013). Dominio de control
Elaborado por: William Chacón

### 1.8.3. ITIL V3

Es un conjunto de buenas prácticas para mejorar la gestión, procedimientos, roles, tareas y responsabilidades que se puedan adaptar a cualquier organización de TI, con la finalidad de ayudar a lograr la calidad y eficiencia en las operaciones de TI (Milenium, 2008).

El objetivo principal es satisfacer las necesidades sin asumir directamente las capacidades y recursos necesarios para ello (ITIL V3, 2011).

Para realizar una correcta gestión en una organización se debe tomar en cuenta los siguientes puntos:

- Conocer las necesidades del cliente.
- Estimar la capacidad y recursos necesarios para la prestación del servicio.
- Establecer los niveles de calidad de servicio.
- Supervisar la prestación del servicio.
- Establecer mecanismos de mejora y evolución del servicio.

Como se puede apreciar para mejorar la gestión en una organización TI se deberá establecer mecanismos internos para reducir los riesgos de seguridad informática.

ITIL V3 tiene 5 fases del ciclo de vida de los servicios de TI, el cual se detalla a continuación:

1. **Estrategia para los servicios de TI**

   Es el eje central para que las siguientes fases se ajusten a las políticas y estrategias del negocio, con el objetivo de determinar en primera instancia qué servicios deben ser prestados y porqué han de ser prestados desde la perspectiva del cliente y el mercado.

   Para realizar una correcta estrategia de un servicio se debe tomar en cuenta los siguientes puntos:

   - Conocer el mercado y los servicios de la competencia.

- Proponer servicios diferenciados que aporten valor añadido al cliente.
- Gestionar los recursos y capacidades necesarios para prestar los servicios ofrecidos al cliente.
- Alinear los servicios con la estrategia del negocio (ITIL V3, 2011).

**2. Diseño de los servicios de TI**

Esta fase permite diseñar nuevos servicios o modificar los ya existentes para su incorporación en el catálogo de servicios para su posterior paso a producción.

En la fase del diseño del servicio se debe tomar en cuenta todos los requisitos y recursos del servicio para que la operación sea eficiente y evitar una mala imagen en el mercado de organizaciones IT (ITIL V3, 2011).

**3. Transición de los servicios de TI**

Esta fase hace que los productos o servicios definidos en la fase de diseño se integren en un entorno de producción y sean accesibles a los usuarios, las funciones principales que se debe realizar en la etapa de transición son:

- Garantizar que los nuevos servicios se cumplan.
- Mejorar la satisfacción del cliente respecto a los servicios prestados brindando un valor agregado.

Para cumplir con estas funciones se debe planificar todo el proceso de transición o cambio para garantizar al cliente la operación del nuevo servicio a los parámetros definidos y por ende luego de un determinado tiempo el cliente podrá observar claramente la mejora del servicio en función a las necesidades del negocio (ITIL V3, 2011).

**4. Operación de los servicios de TI**

Es la fase en donde se puede apreciar claramente la gestión de los servicios prestados y acordados mediante niveles de calidad.

La fase de operación del servicio refleja la gestión realizada en las anteriores fases, es evidente que de nada servirá si no se realizó una correcta estrategia, diseño, transición; si el servicio prestado falla y no se entrega un servicio de calidad acordado con el cliente (ITIL V3, 2011).

### 5. Proceso de mejora continua de los servicios de TI

Esta fase permite incorporar nuevos servicios y mejorar la calidad de todos los procesos y actividades en la prestación de servicios TI.

Los objetivos principales de la fase de mejora continua son los siguientes:

- Conocer la calidad y rendimiento del servicio.
- Detectar oportunidades de mejora.
- Brindar recomendaciones de mejora en la gestión IT al cliente.
- Supervisar la implementación.
- Brindar valor agregado e innovador al servicio prestado (ITIL V3, 2011).

Fases de ITIL V3

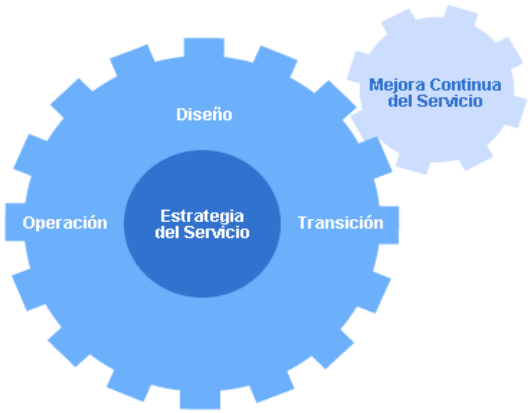



*Figura 6.* Ciclo de vida de ITIL V3
Fuente**:** (ITIL V3, 2011)
Elaborado por: William Chacón

La siguiente tabla es una comparación entre las 3 metodologías o marcos de referencia que se ha decidido utilizar en la elaboración de la presente tesis.

Tabla 2. *Comparación de los marcos de referencia*

| ÁREA | COBIT | ITIL | ISO 27002 |
|---|---|---|---|
| **Funciones** | Mapeo de procesos IT | Mapeo de la gestión de niveles de servicio IT | Marco de referencia de seguridad de información |
| **Áreas** | 4 Procesos y 34 Dominios | 9 procesos | 11 Dominios |
| **Creador** | ISACA | OGC | ISO International Organization for Standardization |
| **¿Para qué se implementa?** | Auditoria de sistemas de información | Gestión de niveles de servicio | Cumplimiento de Estándar de seguridad |
| **¿Quiénes lo evalúan?** | Compañías de contabilidad, Compañías de consultoría IT | Compañías de consultoría en IT | Compañías de consultoría en IT, Empresas de seguridad, Consultores de seguridad en redes |

Nota. (IT GOVERNANCE INSTITUTE, 2008)
Elaborado por: William Chacón

Según la tabla #2 describe la comparación de los marcos de referencia, la justificación y comentarios a nivel internacional, debido a que son cada una necesaria al momento de un análisis de situación actual.

## 1.9. Estudio de herramientas de análisis para la prevención de vulnerabilidades

### 1.9.1. Herramientas y técnicas para la auditoria informática

1. **Encuestas**

Es una herramienta útil para la recolección de información y documentación.

Este insumo es un apoyo para estructurar el informe final del auditor y dependen de la capacidad análisis de este parar determinar las debilidades y fortalezas del entorno.

2. **Entrevistas**

Esta actividad permite interactuar y relacionarse con el auditado. En una entrevista se pueden definir por:

- Requerimiento de documentos puntuales que son utilizados o están bajo la custodia del auditado.

- Entrevistas que no tienen definidos una guía o plan estricto para el levantamiento de información.

- Entrevistas en las que auditor se guía en un proceso preestablecido y buscando obtener información para un fin determinado.

**3. Check List**

"Son cuestionarios predeterminados o elaborados por el auditor con el fin de recolectar una información correcta; en donde, permita encontrar los puntos débiles y fuertes del caso de estudio para su posterior análisis, cruzamiento y síntesis" (Métodos y Técnicas de auditoria informática, 2013).

**4. Tarjeta de observación**

La tarjeta de observación es una técnica que nos permite emitir un criterio personalizado sobre los hechos y acontecimientos más amplios de lo que sucede en una organización.

### 1.9.2. Herramientas y técnicas de informática forense

A continuación se expondrán herramientas de libre distribución que permiten la detección (uso como sistema preventivo) y el rastreo de evidencias (Luego de que se presente un siniestro) con el fin de aplicar las más representativas y así reducir los problemas detectados en el análisis del Service Desk.

Tabla 3. *Herramientas de informática forense*

| Nombre | Descripción | Prevención | Diagnóstico |
|---|---|---|---|
| **F.I.R.E.** | Sirve para realizar análisis, respuesta de incidentes, recuperación de datos, exploración de virus, también proporciona herramienta para el análisis forense. | | X |

| | | | |
|---|---|---|---|
| **ENCASE** | Herramienta para la detección, prevención e investigación de fraude en entornos virtuales.<br>Permite crear copias comprimidas de los discos duros, analizar varias partes de la evidencia, permite ver los archivos borrados, etc. | | X |
| **ByteBack-Tech Assist, Inc** | Copia de discos duros de cualquier formato trasferencia a otros medios internos o externos | | X |
| **SafeBack-New Technologies Inc** | Permite hacer copias espejo de archivos de backups o discos duros completos | X | |
| **WinHex** | Software para informática forense y recuperación de archivos,<br>editor hexadecimal de archivos, discos y RAM | | X |
| **E E-ROL** | Es una aplicación on line que permite a los usuarios recuperar los archivos<br>que hayan sido borrados de unidades de disco duro, unidades Zip en todas las unidades de los sistema operativos de la familia Windows | | X |
| **EasyRecovery** | Recupera datos, archivos, correo electrónico | | X |
| **Snort** | Sistema de prevención y detección<br>de intrusos en la red | X | |
| **Nmap** | Potente localizador de Vulnerabilidades | X | |
| **Nessus** | Escanear vulnerabilidades | X | |
| **Ethereal** | Sniffer para el rastreo de los paquetes de red | X | |
| **Fport** | Identifica puertos abiertos y aplicaciones asociadas a ellos | X | |
| **Putty** | Cliente que utiliza el protocolo de seguridad de SSH | | X |
| **Airsnort** | Herramienta Wireless para recuperar claves cifradas | | X |
| **Aircrack** | Sniffer y web craqueador de Wireless | | X |
| **The Autopsy** | Browser para la informática forense | | X |

| | | |
|---|---|---|
| **Conan** | Revisa vulnerabilidades y emite un informe detallado de los problemas encontrados emitiendo sugerencias para reducir el riesgo | X |
| **Fbackup** | Permite obtener respaldos automáticamente en tiempos programados | X |

Nota. (Belloso Ramiro, 2008)
Elaborado por: (Belloso Ramiro, 2008)

De la tabla #3 se pudo realizar un estudio previo de las herramientas y la funcionalidad de cada una de ellas. Para el análisis y cumplimiento de la red en el Service Desk se usarán las siguientes herramientas:

- Nessus
- Nmap
- Conan

Las herramientas que constan en esta lista ayudarán a realizar la detección de posibles vulnerabilidades con el fin de corregirlas y reducir el posible riesgo en el Service Desk.

Adicional se utilizará una herramienta de Windows complementaria llamada MBSA (Microsof Baseline Security Analizer). La misma nos emite un informe de vulnerabilidades y las recomendaciones para reducir el riesgo en las estaciones de trabajo. (Microsoft, 2015)

Las otras herramientas no han sido tomadas en cuenta debido a que son utilizadas para rastrear evidencias es decir cuando ha ocurrido un problema informático es por eso que el objetivo de la presente tesis es tener un panorama preventivo en función a la situación actual del Service Desk.

### 1.9.3. Nessus

Nessus es un programa que permite detectar vulnerabilidades mediante una interfaz web; Así también, permite escanear y buscar puertos abiertos en los equipos de red.

Al finalizar el proceso este programa genera un reporte con las anomalías que pueden existir en los equipos si fuese el caso; este resultado brinda un panorama al personal técnico de soporte o administrador de la situación de los equipos del caso de estudio, verificando si existen novedades este pueda tomar las acciones pertinentes para minimizar los riesgos de seguridad.

Los resultados del análisis de programa Nessus se pueden exportar a varios formatos de archivo, lo que permite almacenarlos para generar una base de conocimiento de las anomalías encontradas.

Seguidamente se muestra la tabla de criticidad de vulnerabilidades de acuerdo al color que despliega el informe de la herramienta.

Tabla 4. *Criticidad de vulnerabilidades*

| Color | Severidad |
|---|---|
| Morado | Crítica |
| Rojo | Alto |
| palo de rosa | Alto |
| Naranja | Medio |
| Azul | Bajo |
| Verde | Información |

Nota. Tabla de criticidad al emitir el reporte de Nessus
Elaborado por: William Chacón

A continuación se detalla algunas vulnerabilidades que puede encontrar Nessus:

1. **Desbordamiento de Buffer**

   Si un programa no controla la cantidad de datos que se copian en buffer, puede llegar un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

2. **Vulnerabilidad de condición de carrera (race condition)**

   Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable que cambia su estado y puede obtener de esta forma un valor no esperado.

### 3. Vulnerabilidad de Cross Site Scripting (XSS)

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

### 4. Vulnerabilidad de denegación del servicio

La denegación de servicio hace que un recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema.

### 5. Vulnerabilidad de ventanas engañosas (Window Spoofing)

Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

Estas vulnerabilidades expuestas son las más comunes que puede detectar Nessus, sin embargo en el análisis de la situación actual del Service Desk se podrá conocer detalladamente cada una de las anomalías.

## 1.9.4. NMAP

Nmap es una herramienta de software libre para explorar, administrar y auditar la seguridad de redes de ordenadores. Detecta host on line, sus puertos abiertos, servicios y aplicaciones corriendo en ellos, su sistema operativo, que firewalls/filtros corren en una red y de qué tipo son. Es excelente para hacer trabajos de auditoria de res y fue diseñado para llevar acabo escaneos rápidos en una gran cantidad de

redes, pero es igualmente usable en hosts individuales. Es reconocido como el scanner de puertos más poderoso. Y se lo usa básicamente para 3 cosas: (Eduardo Federico Santillan, 2010)

- Auditorias de seguridad.
- Pruebas rutinarias de redes.
- Recolector de información para futuros ataques. (Hackers).

"Nmap es software libre y por lo tanto gratuito. Y básicamente existe una versión para cada sistema operativo que conozcas: MacOSX, Microsoft Windows, GNU/Linux, OpenBSD, Solaris, etc." (Eduardo Federico Santillan, 2010).

#### 1.9.4.1. Funcionamiento de Nmap

Soporta escaneos sobre ciertos puertos específicos, entre rangos de IP´s específicos, uso se paquetes Null (retraso en el paquete), FIN (define el bit TCP), Xmas (define los bits de control) y ACK (Confirmación de recepción de mensaje), además SYN (Establece conexión) que es el paquete por defecto. Esto significa que se mandan cierto tipo de paquetes a cada puerto y estos responderán con alguna señal que permitirá a scanner encontrar versiones y servicios. (Eduardo Federico Santillan, 2010)

### 1.9.5. CONAN

Es un programa gratuito que revisa cada una de las vulnerabilidades, y al finalizar nos ofrece un reporte detallado del estado de seguridad del ordenador y las recomendaciones que se deberá seguir en el caso de que la herramienta emita varias observaciones. Adicional permite realizar el escaneo de puertos y servicios en ejecución que nos podría indicar algún malware residente. (Inteco, 2011)

La versión de Conan solo se encuentra disponible para Windows, en la actualidad la herramienta ha sido actualizada con mejores técnicas internas, es decir, ha incorporado nuevas funciones de análisis proporcionando un informe más exhaustivo, además de una mayor usabilidad. (Gambeta, 2011)

> Una vez realizado el análisis y recabada la información del sistema y procesada en los servidores externos aparece un cuadro de dialogo que pregunta si deseamos visualizar el informe. Al aceptar desplegará en el navegador los resultados obtenidos. Información detallada del análisis. (Gambeta, 2011)

El aspecto visual del informe se encuentra estructurado en 3 apartados:

- Datos generales del informe.
- Resumen de análisis.
- Información detallada del análisis.

1. **Datos generales del informe**

   En datos generales muestra la siguiente información: nombre de usuario, número de incidencia, fecha de localización por IP. (Gambeta, 2011)

2. **Resumen de análisis**

   > En resumen del análisis se tiene la evaluación general del sistema, tanto en texto como en forma gráfica las partes del análisis que suponen un riesgo. También informa el porcentaje de elementos que no ha podido clasificar y proporciona algunos consejos. (Gambeta, 2011)

3. **Información detallada del análisis**

   En esta parte muestra de forma detallada la información analizada y el resultado respectivo de cada una de las vulnerabilidades encontradas al ejecutar el análisis. (Gambeta, 2011)

### 1.10. Informática forense para diseño de medidas preventivas

Como se describió anteriormente la informática forense es un estudio de vulnerabilidades o fallas sobre infraestructuras de computación, sistemas

informáticos, estructura de una red, con la finalidad de buscar evidencias que colabore a llevar un caso judicial.

- **¿Para qué sirve como medida preventiva?**

  Como medida preventiva sirve a las empresas para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes. Asimismo, permite detectar las vulnerabilidades de seguridad con el fin de corregirlas. Cuestión que pasa por redactar y elaborar las oportunas políticas sobre uso de los sistemas de información facilitados a los empleados para no atentar contra el derecho a la intimidad de esas personas. (Mota, 2013).

  Uno de los objetivos principales de la informática forense es garantizar la efectividad de las políticas seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información, consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas. Su finalidad es perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se hayan producido (Laura Isabel Sainz Miranda, 2007).

  En conclusión, la informática forense tiene un papel, en primer lugar, como sistema preventivo. Sirve para auditar, mediante la práctica de diversas técnicas para probar que los sistemas de seguridad instalados cumplen con ciertas condiciones básicas de seguridad. Los resultados de las auditorías servirán para poder corregir los errores encontrados y poder mejorar el sistema. Así mismo, lograr la elaboración de políticas de seguridad y uso de los sistemas para mejorar el rendimiento y la seguridad de todo el sistema de información (Ramírez, 2008).

“La informática forense busca prevenir el cometimiento de los delitos apoyándose en la seguridad informática” (Elizabeth, Jácome Ortega Alexandra, 2011).

La informática forense será de gran utilidad y apoyo para la detección de vulnerabilidades; y así darles tratamiento para evitar que en el futuro se convierta en un problema informático.

Al realizar la detección de vulnerabilidades antes de los posibles problemas se podrá realizar un diseño de medidas preventivas apoyándose en la informática forense y los marcos de referencias expuestos (COBIT 4.1, ITIL V3, ISO 27002).

Para el desarrollo de la presente tesis la informática forense servirá como medida preventiva y no correctiva, es decir que se analizará las diferentes brechas en el Service Desk y mediante ello se partirá a realizar el análisis de las mismas con la finalidad de diseñar medidas preventivas y/o políticas de seguridad.

# CAPÍTULO 2
# SITUACIÓN ACTUAL DEL SERVICE DESK

## 2.1. Descripción general del Service Desk

### Introducción

Tata Consultancy Services (TCS) es un proveedor que presta servicios a varias empresas a nivel mundial. La empresa Telefónica Ecuador solicita contratar servicios de mesa de ayuda (Service Desk) a TCS para atender los requerimientos de la compañía; es decir un punto de contacto que pueda resolver las necesidades al presentarse un problema o una petición.

Para la descripción de la situación actual del Service Desk se planifico una entrevista con el líder del proyecto con el fin de conocer los procesos, servicios, estructura organizacional, infraestructura tecnológica que mantiene para cumplir con el servicio solicitado por Telefónica (Véase anexo #2).

En primera instancia se conocerá los servicios que brindan las empresas de manera general y a continuación se detallará la información recolectada mediante la entrevista realizada al líder del proyecto del Service Desk de la empresa TATA.

### 2.1.1. “Telefónica” Ecuador

Telefónica es uno de los proveedores más grandes en Ecuador de servicios de telefonía móvil, por lo que se ha visto en la obligación de revisar y/o mejorar la atención y el servicio al cliente, con la finalidad de mejorar los tiempos de respuesta en la solución de problemas de tecnología de manera inmediata y cumplir con las metas establecidas.

Debido al alto crecimiento que ha tenido la empresa en los últimos años, ha visto la necesidad de firmar acuerdos de servicios con la empresa TCS (Servicios de soporte técnico y Help Desk).

En el caso de TCS ha permitido a Telefónica la creación de un entorno de apoyo abierto a sus usuarios y/o proveedores al proporcionar una solución de centro de

atención telefónica para resolver demandas de soporte y apoyo, es decir, un único punto de contacto para responder a sus necesidades durante las 24 horas del día, los siete días de la semana.

### 2.1.2. "TATA" Ecuador

En Ecuador es una de las compañías más grandes en brindar servicios de Tecnología y BPO (Business Process Outsourcing ) ya sea a clientes externos o personal interno de la empresa, es reconocida por los costos que ofrece en el mercado y además por la eficiencia y eficacia que brinda el servicio ofrecido.

TCS ofrece una amplia cartera de negocios que se divide en un portafolio de servicios brindando soluciones de TI, consultoría, servicios de ingeniería y servicios de infraestructura TI.

La operación en Ecuador ha incrementado su oferta. Hoy en día en el país la mayor empresa de BPO a través de la automatización y mejoramiento de procesos operativos y de negocio basados en plataformas tecnológicas y administración global de servicios. Su centro de servicios de BPO cuenta además con sus unidades de negocio de Help Desk y Call Center, entre las más grandes de América. Además ofrece sus servicios tecnológicos de infraestructura tecnológica y consultoría de negocios exitosamente en las estrategias basadas en las mejores prácticas (ITIL), mejorando la eficiencia de los clientes.

### 2.1.3. Ubicación geográfica

Debido al cambio de proveedor, la empresa TCS se ve en la necesidad de ampliar y mejorar las instalaciones con el objetivo de prestar un mejor servicio, debido a este cambio el Service Desk se ve obligado a implantar sus propias instalaciones cerca de las oficinas del cliente para tener un contacto directo, y así tener establecido el soporte de una manera eficaz, rápida y oportuna.

Ubicación geográfica

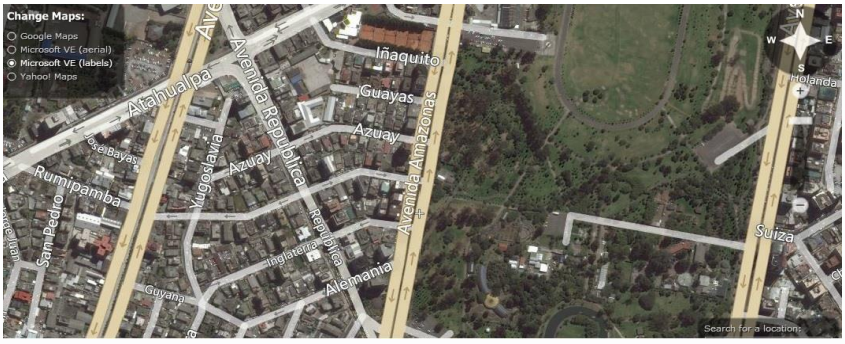



*Figura 7.* Ubicación geográfica del Service Desk
Fuente: Líder del proyecto
Elaborado por: William Chacón

### 2.1.4. Estructura organizacional

La empresa TCS tiene establecido sus funciones y obligaciones mediante una estructura organizacional, en el cual está ocupado por cargos dependiendo sus labores dentro de la organización de los proyectos y servicios que presta la empresa. (Véase anexo 1)

### 2.1.5. Service Desk

El nombre de Service Desk (Mesa de ayuda) es conocido mediante términos y lineamientos de ITIL, con la finalidad de gestionar y solucionar todas las incidencias y/o requerimientos reportados por el cliente siguiendo un proceso establecido.

Para brindar la atención se pueden usar varios canales de comunicación: extensiones de telefonía, portal de autogestión, correo electrónico, mensajería instantánea, para así entregar asistencia que puede ser a personal interno a la organización, proveedores, consultores entre otros; y el Service Desk deberá entregar la información oportuna a los usuarios que pueden gozar del servicio.

Por lo tanto para brindar el servicio de Service Desk se dividen en 5 grupos específicos.

1. Grupo de Servicios “Call Taker”
2. Grupo de Servicios “Soporte de Aplicaciones”
   2.1.Grupo de servicios “Recargas Electrónicas”

2.2.Grupo de servicios “Proyectos Especiales”

3. Grupo de Servicios “Gestión de Puesto de Trabajo”

## 1. Grupo de Servicios “Call Taker”

El grupo de servicios de Call Taker tiene como objetivo ser el único punto de comunicación del área de Tecnología de Telefónica y los usuarios. Como parte de esta función, la empresa TCS deberá registrar, acompañar, realizar el seguimiento y solucionar los reclamos y solicitudes de servicio de los usuarios.

El Call Taker recibirá todas las llamadas de los usuarios internos y externos que deseen reportar incidencias o peticiones de los servicios que brinda la Vicepresidencia de Tecnología y será responsable de su correcta atención, diagnóstico y derivación del caso.

Además se encargará de gestionar los requerimientos recibidos mediante correo y portal web, siendo estos canales con menor demanda para el Call Taker pero que forman parte de los medios de atención de incidentes y peticiones de servicio.

El servicio comprende la disposición del personal para la atención de las llamadas, correos y tickets abiertos por el portal que requieran la atención del Call Taker, análisis de primera línea, así como también, la provisión de toda la infraestructura física y tecnológica necesaria para la recepción, atención, escalamiento de llamadas y tickets a otros grupos resolutorios.

Los servicios más comunes que prestan el grupo de Call Taker son los siguientes:

- **Asistencia Remota**

El soporte Remoto permite al usuario contactarse directamente con el ejecutivo de Call Taker con la finalidad de verificar las actividades del usuario que realizo en su computador o implementar requerimientos nuevos, esto en cuanto a un tiempo determinado y establecido por el cliente.

Proceso de Call Tacker


*Figura 8.* Diagrama de solución de soporte Call Taker
Fuente: Líder del proyecto
Elaborado por: William Chacón

## 2. Grupo de Servicios "Soporte de Aplicaciones"

El grupo de servicios de soporte de aplicaciones dan respuesta a los tickets abiertos por las diferentes áreas de la empresa, que involucran algún tipo de inconveniente con las aplicaciones y plataformas de TI administradas por tecnología que utilizan los clientes internos para dar servicio a los abonados de Telefónica.

El soporte de aplicaciones de TI recibirá todos los requerimientos de los usuarios por derivación directa del Call Taker y/o se generen por las herramientas de autogestión o los buzones de correo asignados para este grupo de servicios.

Como parte de este servicio, El grupo de soporte deberá registrar, acompañar, realizar el seguimiento y solucionar los reclamos y solicitudes de servicio de los usuarios.

Actualmente los tickets abiertos por los usuarios son reportados al Call Taker a través de tres canales:

Canal telefónico, vía correo electrónico dirigido al buzón del Call Taker o son abiertos directamente a través del portal de autogestión, este último canal permite la creación de la petición automática y así pueda ser solucionada el requerimiento por el área de soporte adecuada dando un análisis previo por el primer nivel de soporte.

Proceso del grupo aplicaciones

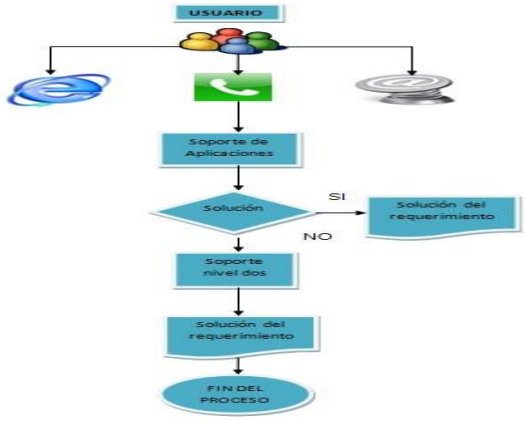



*Figura 9.* Diagrama de solución de soporte aplicaciones
Fuente: Líder del proyecto
Elaborado por: William Chacón

### 3. Grupo de Servicios Gestión de Puesto de Trabajo

El Grupo de servicio de soporte en sitio, recibirá todas las solicitudes de los usuarios internos y externos que se reciban por derivación directa del Call Taker y que no hayan podido ser resueltas en el contacto telefónico con el usuario que reporta el requerimiento.

El Call Taker deriva al grupo de soporte en sitio todos los requerimientos que no puedan ser solucionados en primera línea, adjuntando las validaciones realizadas, el ingeniero de soporte se acerca al sitio de trabajo, y el caso sea resuelto o derivado al área correspondiente para su respectivo análisis.

El grupo de gestión de soporte en sitio realiza los siguientes servicios:

1. **Mantenimiento de software**

- **Mantenimiento correctivo**

Este se encarga de realizar las modificaciones de un producto de software después de la entrega, para corregir errores, vulnerabilidades, mejorar el rendimiento del software, eficiencia y otros atributos que pudieron ser omitidos en la construcción del producto.

- **Mantenimiento preventivo**

Además el grupo de soporte en sitio es el encargado de realizar el mantenimiento preventivo, consiste en una atención constante de limpieza, revisión y afinación de los distintos elementos integrantes de un equipo de cómputo. Es importante conocer que la mayoría de los problemas que se presentan en el trabajo diario, se debe a la falta de un programa específico de mantenimiento de los equipos, de tal manera que la mayoría de los problemas se resuelven con el mismo procedimiento del mantenimiento preventivo.

El mantenimiento tiene técnicas para darle un periodo de vida útil más largo y libre de fallas. Debemos de tener en cuenta que es necesario darle mantenimiento al software ya que el continuo uso genera una serie de cambios en la configuración original del sistema, causando bajas en el rendimiento que al acumularse con el tiempo pueden generar problemas serios como pérdida de información importante que involucre al correcto funcionamiento del servicio.

2. **Mantenimiento de hardware**

- **Mantenimiento Correctivo**

El servicio que brinda el soporte en sitio es una serie de rutinas periódicas que debemos realizar en la PC, estas son necesarias para obtener un rendimiento óptimo y eficaz a la hora de su funcionamiento.

- **Mantenimiento preventivo**

Este tipo de mantenimiento consiste en arreglar las partes de un ordenador antes que empiece a fallar o deje de funcionar correctamente, uno de los mantenimientos preventivos principales es la limpieza correcta de las piezas de un ordenador.

- **Gestión y mantenimiento de impresoras**

El servicio que se brinda en impresoras es principalmente el mantenimiento para que no ocurran problemas al momento de usar este dispositivo.

- **Gestión de Inventarios**

La gestión de inventarios se encarga particularmente de llevar un control determinado de los dispositivos que son utilizados por el usuario y así poder conocer más detalladamente a quién corresponde cada equipo.

- **Soporte Remoto**

El soporte Remoto permite al usuario contactar directamente con personal de soporte en sitio y que el agente pueda acceder y ver de forma remota el equipo y las actividades del usuario.

- **Distribución de software y hardware**

El servicio brindado se encuentra establecido a nivel de software en la instalación, modificación o desinstalación de una aplicación propia del cliente, en el caso de que se necesita software externo tendrá que ser analizado por departamento de seguridad de información del cliente para prevenir siniestros.

La distribución a nivel de hardware se encarga particularmente de repartir el mismo según las necesidades del usuario y las peticiones de cada uno de las áreas o departamentos de Telefónica.

Proceso del grupo de Desktop

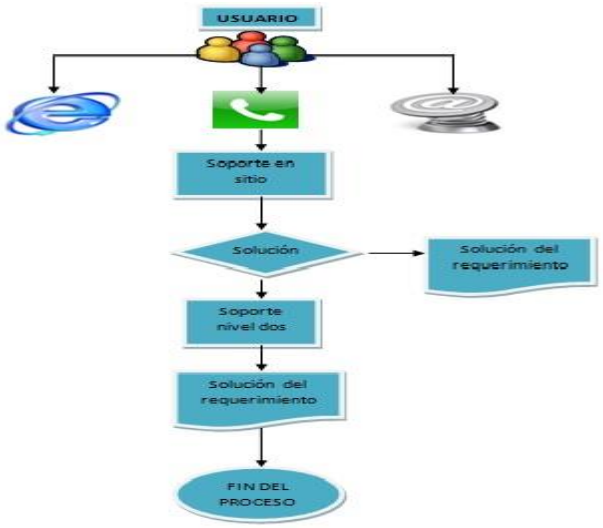



*Figura 10.* Diagrama de solución de soporte en sitio
Fuente: Líder del proyecto
Elaborado por: William Chacón

## 2.2. Descripción y evaluación del entorno informático

El entorno informático es definido un espacio físico en donde se siguen procesos, procedimientos que el personal involucrado debe cumplir, para ello se realizará la descripción y evaluación del entorno con la finalidad de conocer la estructura y el funcionamiento del Service Desk.

### 2.2.1. Arquitectura informática

La arquitectura informática está conformada por la estructura de un sistema informático y la combinación de hardware y software que comunican todos los activos en una red para que cada área trabaje internamente cumpliendo con las funciones del Service Desk, con el fin de brindar soluciones rápidas a los requerimientos del cliente.

Mediante la información que proporcionó el líder del proyecto, se definirá todos los elementos hábiles de hardware y software que se detalla a continuación en la siguiente tabla:

Tabla 5. *Funcionamiento del Service Desk*

| Activo | Descripción |
|---|---|
| Computadores de escritorio | Hardware |
| Laptops | Hardware |
| Elementos de red | Hardware |
| Bases Telefónicas | Hardware |
| Aplicaciones | Software |
| Utilitarios | Software |

**Nota.** Líder del proyecto
**Elaborado por:** William Chacón

### 2.2.2. Entorno de red

El entorno de red es un conjunto de equipos conectados entre sí permitiendo realizar el cambio de información emisor / receptor, por lo tanto el entorno de red del Service Desk permite interactuar con el cliente, donde el usuario dará a conocer las incidencias para que el ejecutivo asignado analice el caso y brinde una solución.

El entorno de red está diseñado con la técnica de mantener redundancia; y si por algún motivo; dejara de funcionar o colapsar algún enlace, inmediatamente otro tendría que ocupar su lugar para realizar las tareas del anterior sin ninguna afectación.

La infraestructura de la red se encuentra configurada con los siguientes dispositivos:

Un switch Cisco administrador que determina la función de redundancia cuando amerite el caso, dos switchs Cisco Catalyst 2960 configurados para brindar conexión a las estaciones de trabajo.

Switch Service Desk

*Figura 11.* Switch Cisco Catalyst 2960
Fuente: Service Desk
Elaborado por: William Chacón

### 3. Enrutamiento

El enrutamiento nos permitirá transferir información desde Telefónica hacia Tata Consultancy Services o viceversa, el protocolo de enrutamiento configurado es EIGRP (Protocolo de enrutamiento de Gateway interior mejorado), y el direccionamiento IP establecido es estático.

El Router configurado directamente con el switch administrador es monitoreado por el proveedor Te Uno que se encarga del correcto funcionamiento, confiabilidad, disponibilidad y redundancia de los dispositivos.

### 4. Firewall

El firewall principal del data center externo es el que administra todas las políticas establecidas del tráfico de entrada y salida de información de la red interna de Tata Consultancy Services en el edificio Pucará, por tal razón la red LAN es administrada directamente de las oficinas matriz.

En la red interna de TCS se encuentra configurado 2 firewalls de marca HP Proliant DL380 con varias reglas establecidas por los administradores de la red con el fin de tener niveles de acceso a cada una de las aplicaciones propias del cliente.

### 5. Direccionamiento

La red interna de TCS se encuentra establecida con una red de clase A 10.112.140.0 con direccionamiento estático y distribuida en Vlans; las IP`s de las estaciones de trabajo están estructuradas de acuerdas a las mismas.

A continuación se mostrara la estructura global de la comunicación que se mantiene con el cliente:

Estructura de red

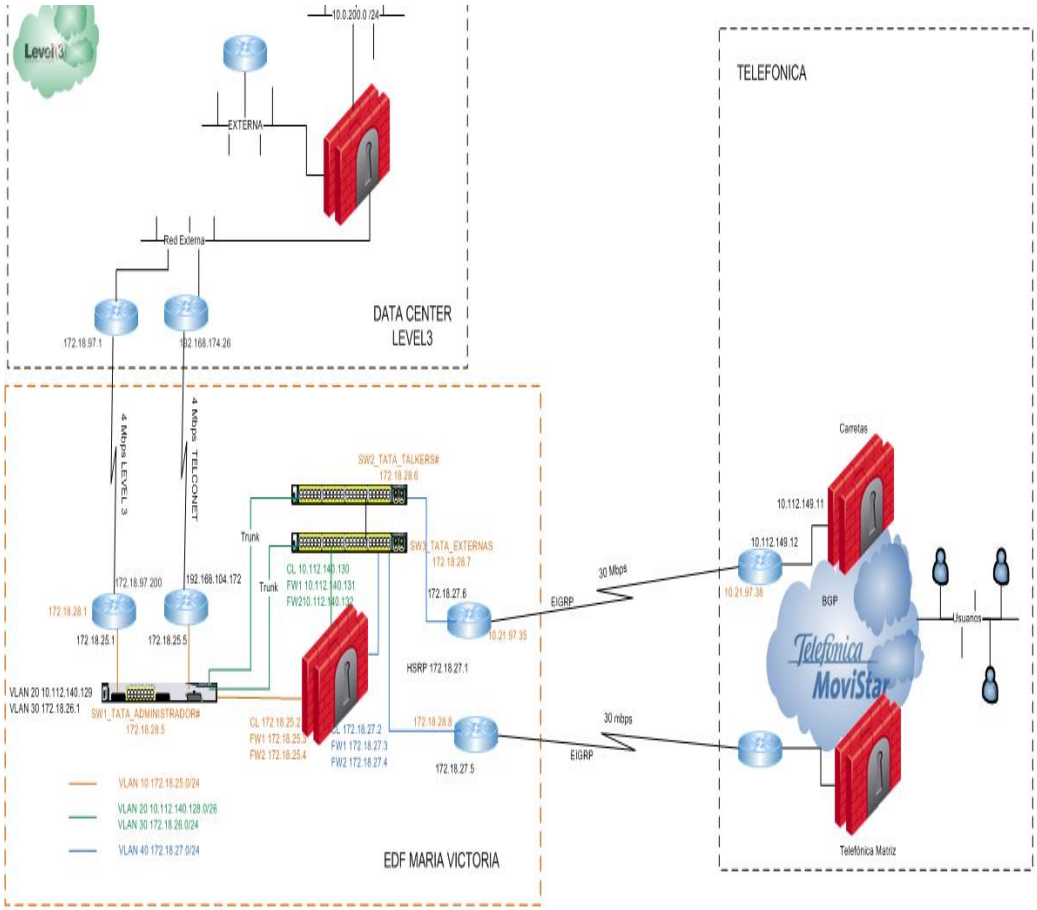



*Figura 12.* Diseño de red
Fuente: Administrador de red TCS
Elaborado por: Nelly Suntaxy

El direccionamiento del Service Desk tiene como estándar el protocolo TCP/IP, y se encuentra en el segmento 10.112.140.128 / 26 como se detalla a continuación:

Tabla 6. *Direccionamiento Ip Service Desk*

| # | IPS | DESCRIPCION USO | GATEWAY | MASCARA DE SUBRED |
|---|---|---|---|---|
| **1** | 10.112.140.136 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **2** | 10.112.140.137 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **3** | 10.112.140.138 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **4** | 10.112.140.139 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **5** | 10.112.140.141 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **6** | 10.112.140.142 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **7** | 10.112.140.145 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **8** | 10.112.140.146 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **9** | 10.112.140.147 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **10** | 10.112.140.148 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **11** | 10.112.140.149 | CALL TAKER | 10.112.140.131 | 255.255.255.192 |
| **12** | 10.112.140.162 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **13** | 10.112.140.163 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **14** | 10.112.140.164 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **15** | 10.112.140.165 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **16** | 10.112.140.166 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **17** | 10.112.140.167 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **18** | 10.112.140.171 | DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **19** | 10.112.140.181 | PRUEBAS DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **20** | 10.112.140.182 | PRUEBAS DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **21** | 10.112.140.183 | PRUEBAS DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **22** | 10.112.140.184 | PRUEBAS DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **23** | 10.112.140.185 | PRUEBAS DESKTOP | 10.112.140.131 | 255.255.255.192 |
| **24** | 10.112.140.168 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **25** | 10.112.140.169 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **26** | 10.112.140.170 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **27** | 10.112.140.173 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **28** | 10.112.140.174 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **29** | 10.112.140.180 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **30** | 10.112.140.151 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **31** | 10.112.140.152 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **32** | 10.112.140.153 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **33** | 10.112.140.154 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **34** | 10.112.140.155 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **35** | 10.112.140.156 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |

| | | | | |
|---|---|---|---|---|
| **36** | 10.112.140.157 | APLICACIONES | 10.112.140.131 | 255.255.255.192 |
| **37** | 10.112.140.158 | PROYECT LÍDER | 10.112.140.131 | 255.255.255.192 |
| **38** | 10.112.97.14 | PROYECT MANAGER | 10.112.140.131 | 255.255.255.192 |
| **39** | 10.112.140.150 | SERVIDOR CCPULSE | 10.112.140.131 | 255.255.255.192 |
| **39** | 192.168.0.1 | SERVIDOR ALTIRIS | 192.168.0.1 | 255.255.255.0 |

Nota. Departamento de red
Elaborado por: William Chacón

### 2.2.3. Aplicaciones

Las aplicaciones que usa el personal del Service Desk son propias de TCS y Telefónica, es decir para brindar el soporte a los usuarios internos (cliente) se debe conocer cada una de las plataformas con la finalidad de brindar un soporte N1.

Las aplicaciones usadas son las siguientes:

Remedy: aplicación utilizada para realizar la gestión de tickets: Escalamientos, asignaciones, cierre de peticiones y / o soluciones propia de Telefónica y los proveedores que mantiene en producción.

Lotus Notes: herramienta interna de TCS para la gestión de los correos electrónicos.

TOAD: aplicación de desarrollo de sentencias SLQ administración de base de datos.

Aplicaciones de servicio al cliente: son usadas por el personal de servicio al cliente de telefónica para realizar consultas de: estado de línea, nombre, cédula, teléfono u otros.

Outlook: aplicación utilizada para realizar la gestión y soluciones que solicita el cliente.

Active Directory: herramienta que permite realizar la gestión de los usuarios, administración de contraseñas, permisos, administraciones.

Ccpulse: herramienta que permite realizar el monitoreo del ingreso de llamadas, tiempo promedio de duración y las llamadas en espera del cliente.

Acronix: aplicación que permite realizar la recuperación de imágenes, restauración, particiones de discos duros y preparación de nuevas imágenes.

### 2.2.4. Uso de los marcos de referencia en el Service Desk de Telefónica

- **Uso de COBIT en el Service Desk de Telefónica**

Como se ha descrito COBIT es un marco de referencia o metodología de mejores prácticas orientada a procesos, procedimientos y actividades alineadas al negocio de TI, en el caso del Service Desk se oferta un servicio N1 de apoyo al cliente en asistencia y resolución de ticket, para lo cual se debería definir procesos y procedimientos que ayuden al cumplimiento del objetivo principal del negocio, brindar el servicio de soporte y apoyo.

Los procedimientos no solo aplican a los procesos administrativos sino también a los que TCS brinda en cada uno de los proyectos existentes, por lo tanto los procedimientos deberían estar definidos según el proyecto, área y objetivos internos.

El proyecto del Service Desk debe alinearse a un reglamento interno que es el de TCS y aun externo que es el de Telefónica, por lo tanto sus procedimientos deben ser revisados y analizados en función del cumplimiento al objetivo principal que como proyecto se tiene que es el brindar un servicio de soporte, asistencia y resolución de tickets a Telefónica, los procesos que existan deben tener controles y definir actividades para el cumplimiento de procedimientos internos del servicio y deben ser revisados y aprobados por la alta gerencia, todo esto en función de lo que indica COBIT en su marco teórico de la metodología orientada a procesos. Es decir el análisis de los procedimientos y el cumplimiento de los mismos serán analizados con el marco de referencia descrito.

- **Uso de ISO 27002 en el Service Desk de Telefónica**

Por definición sabemos que se debe dar la mayor seguridad a la información ya que se ha convertido en el principal activo de las empresas, por lo tanto se ha

definido que los aspectos analizar con la norma ISO 27002 serán: red interna, instalaciones y el grado de madurez de los procedimientos.

La norma ISO 27002 contiene Dominios de control bien definidos que permitirá mejorar la administración y gestión de la red así mismo sobre la seguridad de las instalaciones del Service Desk y el cumplimiento de políticas y procedimientos.

Como se explicó anteriormente las mejores prácticas de ISO 27002 han sido definidas para mejorar la gestión de la seguridad de la información. Al ser Tata Consultancy Services una empresa que presta servicios de TI y soporte, se ve en la necesidad de analizar brechas internas en el servicio de mesa de ayuda (Service Desk) que permita mejorar la gestión de la información manejada en la red Cliente – Proveedor.

- **Uso de ITIL en el Service Desk de Telefónica**

Por lo revisado anteriormente se define a ITIL como una metodología orientada a la mejora continua de servicios, TCS como empresa busca siempre que sus empleados cumplan con lo que manda la normativa es por ello que se ha incluido cursos de capacitación y certificación de la norma ITIL.

Para usos del análisis de la situación actual del Service Desk se utilizará ITIL para validar el personal ya que son parte fundamental del servicio, adicional a esto las mejores prácticas de ITIL son principalmente orientadas a los servicios de apoyo y soporte como lo es el proyecto del Service Desk de Telefónica.

El momento de la revisión se tomará en cuenta el ciclo de vida de ITIL que norma desde el manejo de incidentes hasta la mejora continua entonces se verificará si el personal de TCS que presta el servicio se encuentra en conocimiento de lo que el cliente solicita y de lo que manda la norma de ITIL.

Ya que el alcance de la presente tesis se encuentra abarcando procesos, personas, instalaciones y redes, se ha definido el uso de cada marco referencial según su orientación más definida y reconocida especialmente por ISACA institución que

norma a nivel internacional la forma de revisión o auditoria de sistemas en organizaciones públicas o privadas sin importar su tamaño.

## 2.3. Investigación de campo

### 2.3.1. Introducción

"La investigación de campo es la técnica de recolección de datos directamente del lugar o realidad donde ocurren los hechos sin manipular, alterar variables algunas con el fin de comprender, resolver alguna situación necesidad o problema en un contexto determinado." (Fidias Arias, 2004)

El investigador que la aplica debe trabajar en el ambiente natural en que conviven las personas o en el que las fuentes consultadas se desenvuelven, para obtener los datos más relevantes a ser analizados.

Objetivos de la investigación de campo

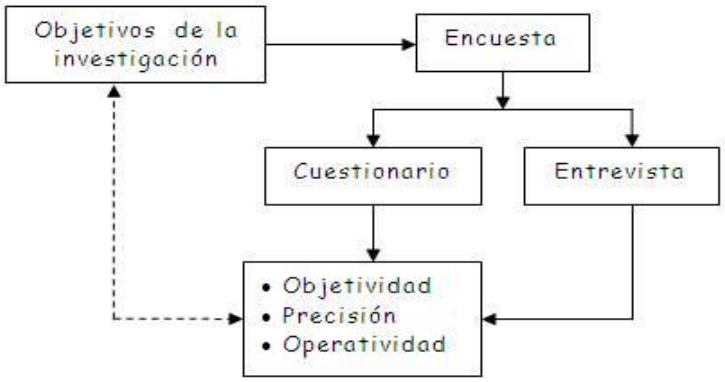



*Figura 13.* Mapa conceptual del uso de herramientas para investigación de campo
Fuente: (Fidias Arias, 2004)
Elaborado por: William Chacón

Para el levantamiento de información en el Service Desk se ha creado encuestas y Check List que fueron publicadas en el internet mediante la herramienta EncuestaTick y enviada al personal para que pueda resolver la encuesta. El link de la herramienta es el siguiente: http://www.portaldeencuestas.com/index.php.

A continuación se detallará paso a paso las herramientas utilizadas para el análisis de la situación actual.

### 2.3.2. Encuestas en el Service Desk

Como se define en el capítulo 1, la encuesta es una herramienta útil para la recolección de información y documentación. Partiendo de este punto se realizó la elaboración de una encuesta con el objetivo de conocer el cumplimiento de las políticas de seguridad de información, una vez elaborada la encuesta se realizó la codificación de la misma es decir se brindó una codificación o nomenclatura a la encuesta.

El código de la encuesta es ENC001, la misma fue publicada en el internet mediante la herramienta EncuestaTick y enviada al personal para que pueda resolver la encuesta.

Se tiene un total de 32 encuestas resueltas por el personal de las 3 áreas del Service Desk, (Véase en anexo #3), el mismo es el formato de encuesta utilizado para la recopilación de información para el personal interno del proyecto.

### 2.3.3. Entrevistas en el Service Desk

De lo definido en el capítulo 1, la entrevista permite interactuar y relacionarse con el auditado.

Tomando en cuenta el uso de la herramienta se elabora dos entrevistas para la obtención de información directa con respecto a temas importantes para la resolución de la presente tesis, la primera entrevista en inicio está dirigida solo al administrador de la red interna del proyecto, por temas de revisión y organización interna de TCS se realiza la misma entrevista al ingeniero de seguridad a cargo de la red interna del proyecto, la segunda entrevista fue dirigida al personal que hace sus funciones de jefes de área y al líder de proyecto Service Desk.

Las codificaciones de las entrevistas son las siguientes:

1. **ENT001:** permite identificar los controles de seguridad existentes de la red interna del Service Desk.

2. **ENT002:** permite conocer los procedimientos establecidos en la organización.

### 2.3.4. Entrevista Red interna ENT001

El objetivo de la entrevista es conocer la administración, monitoreo, y seguridad de la red interna del proyecto. La entrevista fue elaborada con preguntas sacadas del marco de referencia para análisis ISO 27002 en el objetivo de control 10.6 (Véase anexo 11). Se toma criterios del marco de referencia que deben estar presentes en una red interna, la entrevista en inicio fue dirigida y realizada con la administradora de la red interna que es parte del personal de arquitectura de TCS, luego de esta entrevista se pudo identificar que se debía hacer un acercamiento con el personal de seguridad informática de TCS por lo que la entrevista tubo dos etapas la de la administración y la de seguridad.

A continuación se muestra la documentación realizada para cada entrevista de la red interna:

**Entrevista gestión de seguridad de las redes ENT001**

**Entrevistado:** Administrador de red
**Responsable:** Henry Chacón
**Fecha:** 08 de Enero 2015
**Temas tratados:** Red interna del Service Desk de TATA para Telefónica.

**Objetivo de la entrevista:**

La entrevista tiene como objetivo conocer la administración y manejo actual de la Red Interna del Service Desk de TATA para TELEFÓNICA.

1. **¿Qué tipo de controles y seguridades están aplicándose a la red interna para controlar el tráfico de información y la información que por ella transita?**

   Se mantiene definidos controles de velocidad en la información, también se ha determinado hora de tráfico en las que se puede tener mayor afectación con lo cual se ha realizado configuraciones necesarias para segregar el tráfico.

   Las seguridades han sido definidas por contrato y según los Hardening existentes para seguridad en redes de TCS.

2. **¿Qué procedimientos están vigentes para la toma de control a máquinas internas que pertenecen a la red de la mesa de ayuda?**

   Se mantiene definida una política de toma de control en la que está prohibida la toma de control de máquinas de la mesa de ayuda desde el exterior, por salvaguardar la información que en ellas pueda existir, así como se tiene controles para la instalación de programas que puedan hacer posible esta acción, solo existen excepciones para la toma de control en caso de que se trate de personal con cargo de jefaturas y sea necesaria la tarea de toma de control.

3. **¿Qué tipo de controles, procedimientos y configuraciones están vigentes para conexiones de tipo inalámbricas a la red interna?**

   Existe un procedimiento interno de TCS que se cumple para conexiones inalámbricas, el usuario debe hacer registrar su equipo en gestión de identidades quien a su vez solicita en control de cambios se otorgue los accesos inalámbricos de los usuarios.

4. **¿Qué políticas de servicio y seguridad de la red interna están vigentes?**

   Una política como tal no se encuentra vigente ya que Telefónica como cliente no ha hecho conocer ninguna política, lo que se mantiene vigente es el Hardening de red interna, que es un documento tipo procedimiento en el que

se cuenta con puntos de seguridad básicos que se debe cumplir el momento de una implementación de red interna.

5. **¿Qué procedimientos se encuentran vigentes para restringir el acceso a los servicios de red y /o aplicaciones?**

   Los procedimientos para accesos son internos y propios de TCS, cada acceso debe estar aprobado por el área de seguridad informática con gestión de identidades, esto para cuando se trata de aplicaciones internas de TCS, si se trata de aplicaciones del cliente pues se deberá cumplir con lo que indique en este caso Telefónica.

6. **¿Se mantiene tecnología aplicada de seguridad de los servicios de red como: autenticación, encriptación y los controles de conexión de red?**

   Se mantiene un registro de logeo a la red y está guardado en log´s de los equipos mediante acciones realizadas, el único log que se mantiene guardado de manera histórica es el de los firewalls, con el tema de encriptación con Telefónica no se ha definido información que cumpla con este requerimiento. (ISO/IEC, 2007)

### 2.3.5. Entrevista Procedimientos ENT002

El objetivo de la entrevista es conocer a nivel de supervisión y jefatura cuanto conocen de los procedimientos existentes para la seguridad de la información y entrega del servicio a Telefónica, y si esta documentación existe o no dentro del proyecto y empresa.

Está dirigida principalmente a las jefaturas de cada área ya que a su nivel deben estar reconocidas para que pueda ser difundida al resto del personal, como jefaturas además deben conocer la importancia de la seguridad de la información definida por el cliente y la empresa, y la documentación existente para la forma de entrega del servicio.

Como parte de la revisión a continuación se presenta la documentación de una de las entrevistas realizadas.

**Entrevista procedimientos de seguridad de información**

**Entrevistado:** Líder del proyecto
**Responsable:** Henry Chacón
**Fecha:** 26 de Diciembre de 2014
**Temas tratados:** Procedimientos de seguridad de información.

**Objetivo de la entrevista:**

El objetivo de la entrevista es identificar la documentación existente como políticas y procedimientos que normen la seguridad de la información.

**PREGUNTAS**

1. **¿Existen políticas emitidas por el cliente Telefónica para la seguridad y manejo de la información dentro del Service Desk?**

   Telefónica como cliente no ha definido políticas de seguridad para sus manuales internos, para el manejo de información de equipos de los usuarios se ha definido documentación que se encuentra disponible para conocimiento del personal de TCS y personal interno de Telefónica.

   La documentación contiene procedimientos a cumplir según el tipo de información que se va a manipular misma que dependerá del usuario custodio de la información.

2. **¿Qué tipo de controles se han definido para el manejo de información del cliente dentro del área del Service Desk?**

   No existen controles definidos para el manejo de información, ya que la información es pública en un compartido.

   Para manejo de información crítica se ha definido por contrato confidencialidad entre las partes, no se ha difundido por ningún medio al

personal la clasificación de información considerada como crítica y la forma de mantener confidencialidad con esta.

3. **¿De qué manera se difunde en el personal la existencia de los controles definidos para la seguridad y manejo de información?**

   La información existente se da a conocer al personal interno mediante correo electrónico con la ruta donde se encuentra alojada la información, mensualmente se realizan reuniones por área para la difusión y validación de que el personal conozca sobre documentación disponible y vigente.

   Como parte de la inducción TCS emite cursos en los que se da conocer el reglamento interno y de seguridad de información a nivel general y que el personal debe cumplir durante su estadía en la empresa.

4. **¿Existe algún proceso que norme el cumplimiento de los controles impuestos?**

   No existe una revisión periódica al cumplimiento de controles impuestos por el cliente y por TCS, la revisión que se realiza es una revisión de rendimiento en función de lo que como operativos han desempeñado en el mes.

5. **¿Se evalúa el conocimiento de los procedimientos con el personal que presta el servicio?**

   TCS cuenta con una página de evaluación continua en la que se debe rendir una prueba de conocimientos de los procedimientos generales de seguridad de información cada año, el curso contiene preguntas de manejo y cuidado de información propia de la empresa y del cliente.

   Adicional a esta evaluación como servicio no se evalúa conocimiento del personal de los procedimientos y políticas entregados por el cliente, toda información o conocimiento se da por sobre entendido en el desempeño de sus funciones.

6. **¿Se ha difundido los controles impuestos por la empresa para la seguridad de información tanto para el cliente como interna?**

   No se ha definido mediante documentación ningún tipo de control para el manejo de información, se difunde el cuidado con el manejo de información de forma verbal entre el personal que brinda el servicio.

7. **¿El cliente realiza revisiones periódicas sobre el manejo de información?**

   El cliente Telefónica no realiza seguimientos del manejo de información, sus revisiones de sus niveles de servicio las realiza de manera mensual, pero en esta revisión no se toma en cuenta el manejo o manipulación de información por parte del proveedor.

8. **¿Dentro de los controles se tiene una clasificación de información? ¿En función de que se la categoriza?**

   TCS tiene definidos categorías para la información considerando su criticidad de datos, es decir el tipo de información que contienen y lo perjudicial que pueden ser en caso de divulgación.

   Como servicio esta documentación en la que se da categorías a la información no se ha difundido entre las jefaturas, su existencia se conoce a través de auditorías realizadas con anterioridad en las que se ha recomendado el uso de home folder, un repositorio de información considerada como confidencial.

9. **¿Se ha definido responsables y custodios de información para salvaguardar la integridad y seguridad de información?**

   Toda información documentada es responsabilidad de los líderes de cada una de las áreas del proyecto así como del líder de proyecto, son los encargados de la difusión en el personal a su cargo y manejo interno de documentación considerada como confidencial o crítica.

10. **¿Existe políticas de seguridad e información que se alineen con los objetivos del negocio?**

    Existen políticas de seguridad indicadas a nivel general independientemente del proyecto que todo el personal de TCS debe cumplir, para una mejora y continuidad del negocio que tiene que ver con la seguridad de información durante la prestación de un servicio tecnológico a empresas de cualquier índole.

11. **¿Están aprobadas y publicadas las políticas de seguridad de información por la alta Gerencia?**

    Se ha definido procedimientos de uso de información aprobados por la alta gerencia que son el Gerente del Servicio y el PM del Servicio, esta información se encuentra disponible para personal autorizado en el home folder.

12. **¿Es revisada por la alta gerencia, las políticas de seguridad de información con intervalos planificados?**

    La reunión para revisión de documentación es solo bajo demanda, no existe periodificación en la revisión de documentación existente o nueva.

13. **¿Es revisada por la alta gerencia, las políticas de seguridad de información en caso que se produzcan cambios significativos?**

    Se realiza una revisión a nivel de alta gerencia, en caso de una nueva documentación o cambio en la documentación existente, esta revisión se la realiza bajo demanda. (ISO/IEC, 2007)

### 2.3.6. Check List de investigación en el Service Desk

Como se mencionó en el capítulo 1 el Check List son cuestionarios predeterminados o elaborados por el auditor con el fin de recolectar una información correcta.

Para la presente tesis se ha utilizado como análisis de información 3 Check List orientados a detectar falencias en los siguientes puntos, instalaciones, Red interna y procedimientos.

Las codificaciones de los Check List son los siguientes:

- **CHL001:** nos ayudará a verificar los controles existentes de red, y la seguridad de los servicios de la red (dirigido al administrador de red).

- **CH002:** permite identificar si el Service Desk mantiene áreas seguras y los equipos se encuentran seguros (dirigido al personal y observación directa).

- **CH003:** permite identificar el grado de madurez de conocimiento de los procedimientos de seguridad (dirigido al personal del Service Desk).

### 2.3.7. Check List red interna CHL001

El Check List de la red interna fue resuelto en sitio y con la intervención del administrador de la red y personal de Seguridad Informática de TCS, quienes como podemos observar más adelante colocaron sus comentarios en cada revisión.

Tabla 7. *Check List de gestión de redes*

| Criterios generales | | | | |
|---|---|---|---|---|
| | SI | No cumple | N/A | OBSERVACIONES |
| ¿Se ha firmado acuerdos de confidencialidad en el manejo, monitoreo y protección de flujo de datos de la red interna del Service Desk de Telefónica? | x | | | Dentro de la firma del contrato por el servicio se define una clausula en la que TCS se compromete a mantener confidencial los datos e información que manejara por el tipo de servicio |

| | | | | |
|---|---|---|---|---|
| ¿El diseño de la red interna cumple con estándares de red reconocidos? | | | | Debe realizarse un análisis respecto a la infraestructura que se requiere pues la red cumple con los lineamientos generales de seguridad con la restricción de acceso a través de firewall y el Hardening disponible para los equipos de comunicación. |
| ¿Se cumple con un proceso de detección de vulnerabilidades en la red interna? | | x | | Este proceso se cumple solo si existe el pedido por parte de PL del proyecto. |
| ¿Se monitorea adecuadamente la red interna del Service Desk de Telefónica? | x | | | El proveedor monitorea la red WAN como parte del servicio de TCS a través de contrato de soporte entre Te UNO y TCS |
| ¿Se cuenta con controles de seguridad implementados en la red interna? | x | | | Firewalls |
| ¿Se ha implementado seguridades en los sistemas y aplicaciones de monitoreo y administración del tránsito de la red interna? | x | | | El monitoreo de la red está a cargo de Te Uno así como la administración y configuración, por lo tanto si se cumple con este requerimiento. |
| ¿En la contratación de servicio se ha definido un acuerdo en el que se defina la gestión de la red interna? | | x | | Dentro de la contratación no se ha especificado este tema pero TCS como empresa cuida la gestión de sus |

| | | | | |
|---|---|---|---|---|
| | | | | enlaces con TE Uno |
| ¿Se ha definido proceso sobre la gestión de red? | | x | | |
| ¿Se ha dado a conocer el procedimiento a seguir en caso de incidentes en la red interna? | | x | | No ha sido factible dado el crecimiento en la localidad y las definiciones técnicas iniciales han sido cambiadas por la necesidad de infraestructura urgente |
| ¿Se tiene definido un plan de contingencia en caso de caída de la red interna? | | x | | A nivel de conectividad , se debe validar la contingencia a nivel de servicio |
| ¿La red interna cuenta con redundancia de enlace al proveedor? | x | | | Con el cliente telefónica la redundancia es manual con dependencia de Telefónica |
| ¿La red interna cuenta con redundancia de conexión interna? | x | | | Únicamente para el core de LAN no disponen de contingencia |

Nota: Administrador de red de Service Desk
Elaborado por: William Chacón

### 2.3.8. Check List de instalaciones CHL002

El Check List de instalaciones fue resuelto por el personal interno y con observación directa sabiendo si cumple o no cumple con las buenas prácticas que norman los marcos de referencia escogidos.

El Check List fue publicado en el internet mediante la herramienta EncuestaTick y enviada al personal para que pueda resolver, se tiene un total de 30 Check List`s resueltos por el personal de las 3 áreas del Service Desk. (Véase anexo #4).

El Check List de observación directa es el siguiente:

## Check List de verificación de cuarto de equipos

**Localidad:** Service Desk (Edificio Pucará piso 1)
**No. usuarios:** 30 Usuarios
**Responsable:** Henry Chacón
**Fecha:** 05/01/2015

**Puntuación:**

| | |
|---|---|
| 4 | Dentro del valor. Cumple con requerimiento |
| 2 | En el límite del valor. Cumple parcialmente con el requerimiento |
| 0 | Fuera del valor. No cumple con el requerimiento o no existe |

***Arquitectura***

| Parámetro | Puntuación | Observaciones |
|---|---|---|
| Cuarto dedicado para equipos | 2 | |
| Dimensión: 4m2 | 2 | |
| Temperatura: 5 a 21°C | 2 | |
| Humedad no condensada: 20 a 55% | 0 | |
| Aire acondicionado | 0 | |
| Ventilación | 0 | |
| Seguridad de acceso | 0 | |
| Piso falso | 0 | |
| Cielo falso | 4 | |
| Canaletas, escalerillas | 2 | |
| Ductos para acometidas | 2 | |
| Punto de voz (ext. telefónica en cuarto de equipos) | 0 | |
| Iluminación adecuada | 0 | |
| Equipos alejados de fuentes de calor (reguladores, baterías de respaldo); campos electrostáticos (transformadores, tableros eléctricos); equipos eléctricos o electrónicos que no sean de comunicaciones y no requieran energía regulada | 0 | UPS cerca de equipos |
| Seguridad contra incendios(plan de evacuación, señalizaciones) | 4 | |
| Seguridad de construcción: No existe riesgo de inundación o filtración de agua(instalaciones agua potable) | 4 | |
| Total | 22 | |

***Requerimientos eléctricos***

| Parámetro | Puntuación | Observaciones |
|---|---|---|
| Más de un acceso o circuito eléctrico para redundancia | 0 | |
| Sistema de transferencia o conmutación de | 2 | |

| | | |
|---|---|---|
| carga | | |
| Generador eléctrico | 2 | |
| Sistema de energía regulada y de respaldo antes cortes (UPS o baterías) | 2 | |
| Topología redundante de UPS | 0 | |
| Soporte de UPS de 60 minutos | 2 | |
| Instalaciones de puesta a Tierra | 2 | |
| Protección de sobrecarga y sobre corriente | 0 | |
| Voltaje Neutro-Tierra: 0.5 Vrms | 0 | NO APLICA |
| Voltaje regulado: 120 V, 60 A | 0 | NO APLICA |
| Transformador de aislamiento en caso de no tener puesta a tierra | 0 | NO APLICA |
| Regleta de tomas reguladas instalada en el rack, sin emplear extensiones o corta picos | 2 | |
| Instalaciones eléctricas soportan carga de equipos de comunicaciones | 2 | |
| La infraestructura cuenta con pararrayos. | 2 | |
| Todos y solo los equipos de comunicaciones están conectados a tomas reguladas | 2 | |
| Total | 18 | |

**Telecomunicaciones**

| Parámetro | Puntuación | Observaciones |
|---|---|---|
| Cableado estructurado cat 5e+ o cat 6 | 4 | |
| Rack de telecomunicaciones de dimensión adecuada:<br>Sucursales: recomendado armario cerrado de 40 unidades (178 cm)<br>Agencias: rack de pared de 19 a 24 unidades (84.55cm a 106.8 cm) | 4 | |
| Bandejas suficientes | 4 | Existen equipos apilados |
| Organizadores de cables | 2 | |
| Protector de línea para conexión de acometida a modem | 2 | |
| Etiquetación de patch panels y face plates | 2 | |
| Etiquetación de patch cords | 2 | No se encuentran etiquetados los cables |
| Rack organizado | 2 | Organizadores sin tapa y cables desordenados |
| Total | 22 | |

| | |
|---|---|
| Seguridad en puertas | 0 |
| Monitoreo de cámaras de seguridad | 4 |
| Seguridad de acceso | 0 |
| Bitácora de acceso | 2 |
| Accesos Alternos | 0 |
| Total | 6 |

| | |
|---|---|
| **Evaluación:** | Arquitectura: Tier 2<br>Eléctrico: No se puede evaluar<br>Telecomunicaciones: Tier 1.<br>Evaluación: Tier 1. No cumple con requerimientos mínimos en la estructura de telecomunicaciones |

### 2.3.9. Check List de procedimientos CHL003

El Check List de revisión de los procedimientos fue elaborado en función de las buenas prácticas y lo normado en los marcos de referencia escogidos, es una evaluación a la calidad de documentación que existe en el proyecto para dar el servicio a Telefónica.

El mismo fue publicado en el internet mediante la herramienta informática EncuestaTick y enviada al personal para que pueda resolver, se tiene un total de 30 Check List`s resueltos por el personal de las 3 áreas del Service Desk. (Véase anexo #5).

### 2.3.10. Observación directa TOB001

Permite tener una lista de chequeo que sirve para registrar todo acto o condición insegura, con el fin de detectarlas, corregirlas y / o controlarlas y prevenir así la ocurrencia de incidentes o vulnerabilidades (Véase anexo #6).

## 2.4. Escenarios de pruebas

Luego de haber realizado la evaluación anterior en el Service Desk, se procederá a determinar varias herramientas de informática forense para el uso en la organización que fueron explicados en el capítulo 1; y mediante los análisis realizados emitir un plan de medidas preventivas para reducir el riesgo que será explicado en el capítulo 3.

Las herramientas a usar son: Nessus, Conan, Nmap.

A continuación se detalla los escenarios que se tomará en cuenta al momento de realizar las pruebas:

- Análisis de puertos abiertos en los equipos del Service Desk de Telefónica.

- Análisis de vulnerabilidades en los Sistemas operativos.

### 2.4.1. Escaneo equipos Call Tacker

A continuación se procederá con el escaneo de vulnerabilidades a todas las IP's de los equipos de Call Tacker, en la tabla que se detalla a continuación se específica el grupo de Ip´s que serán analizadas:

Tabla 8. *IPs Call Tacker*

| | |
|---|---|
| 10.112.140.136 | CALL TAKER |
| 10.112.140.137 | CALL TAKER |
| 10.112.140.138 | CALL TAKER |
| 10.112.140.139 | CALL TAKER |
| 10.112.140.141 | CALL TAKER |
| 10.112.140.142 | CALL TAKER |
| 10.112.140.145 | CALL TAKER |
| 10.112.140.146 | CALL TAKER |
| 10.112.140.147 | CALL TAKER |
| 10.112.140.148 | CALL TAKER |
| 10.112.140.149 | CALL TAKER |

Nota. Administrador de red Service Desk
Elaborado por: William Chacón

Al procesar la información de la lista de IP´s la herramienta de Nessus despliega la siguiente información:

Reporte de vulnerabilidades detectadas en los equipos de Call Tacker


| Plugin ID | Count | Severity | Name | Family |
|---|---|---|---|---|
| 20173 | 1 | Critical | CA Multiple Products Message Queuing Multiple Remote Vulnerabilities | Gain a shell remotely |
| 58435 | 8 | High | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed | Windows |
| 25766 | 1 | High | CA Multiple Products Message Queuing Server (Cam.exe) Remote Overflow | Gain a shell remotely |
| 18405 | 8 | Medium | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness | Windows |
| 57608 | 8 | Medium | SMB Signing Disabled | Misc. |
| 57690 | 8 | Medium | Terminal Services Encryption Level is Medium or Low | Misc. |
| 58453 | 8 | Medium | Terminal Services Doesn't Use Network Level Authentication (NLA) | Misc. |
| 51192 | 7 | Medium | SSL Certificate Cannot Be Trusted | General |
| 57582 | 7 | Medium | SSL Self-Signed Certificate | General |
| 45411 | 4 | Medium | SSL Certificate with Wrong Hostname | General |
| 20840 | 1 | Medium | CA Multiple Products Message Queuing Multiple Remote DoS | Denial of Service |
| 30218 | 8 | Low | Terminal Services Encryption Level is not FIPS-140 Compliant | Misc. |
| 65821 | 5 | Low | SSL RC4 Cipher Suites Supported | General |

*Figura 14.* Reporte de vulnerabilidades detectadas en los equipos de Call Tacker del Service Desk.
Fuente: Nessus
Elaborado por: William Chacón.

La figura 14 nos permite tener una visión de la situación actual de los equipos del Call Tacker. En este caso, se puede apreciar que existen algunas vulnerabilidades definidas en varias categorías de severidad. Es decir, los técnicos deben analizar esta información y si es el caso tomar los correctivos necesarios para solventar el inconveniente.

Con el fin de dar a conocer a detalle la información encontrada en la Figura 14, se darán seguimiento algunas de las alertas con el fin de corregirlas.

- **Severidad crítica**

  En la siguiente figura se muestra el resultado del análisis realizado a la IP 10.112.140.136, la misma muestra que tiene un puerto abierto (4105/TCP). Al realizar el análisis en función del uso de este puerto se puede indicar que de no corregir este inconveniente, este puerto podría ser propenso a un posible riesgo de seguridad.

Severidad crítica

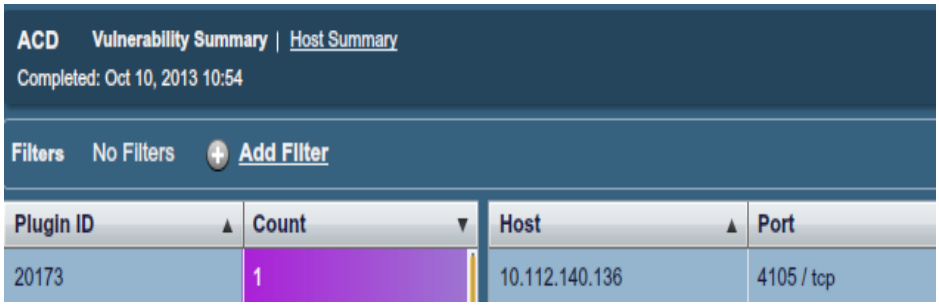



*Figura 15.* Análisis de severidad crítica
Fuente: Nessus
Elaborado por: William Chacón

Esta vulnerabilidad es propensa a un desbordamiento de búfer basado en pila, se puede aprovechar el puerto abierto para ejecutar código arbitrario en algún sistema o aplicación con privilegios de administrador o que sean diferentes para realizar un ataque.

El impacto que puede ocurrir mediante esta vulnerabilidad es afectar a la red y las máquinas del Service Desk mediante el fichero cam.exe dando exposición y libertad a la información confidencial, la pérdida de productividad y la disponibilidad de la red sin necesidad de estar autenticado para explotar esta vulnerabilidad.

Para prevenir esta vulnerabilidad es mantener activado la opción de desbordamientos de búfer en el antivirus del computador.

- **Severidad Alta**

  Ahora se mostrará el informe del análisis presentado por Nessus de las IP´s del Call Tacker; en donde, se puede observar los puertos abiertos en los equipos. Al realizar el análisis en función del uso de este puerto se puede indicar que de no corregir este inconveniente, este puerto podría ser propenso a un posible riesgo de seguridad.

Severidad Alta

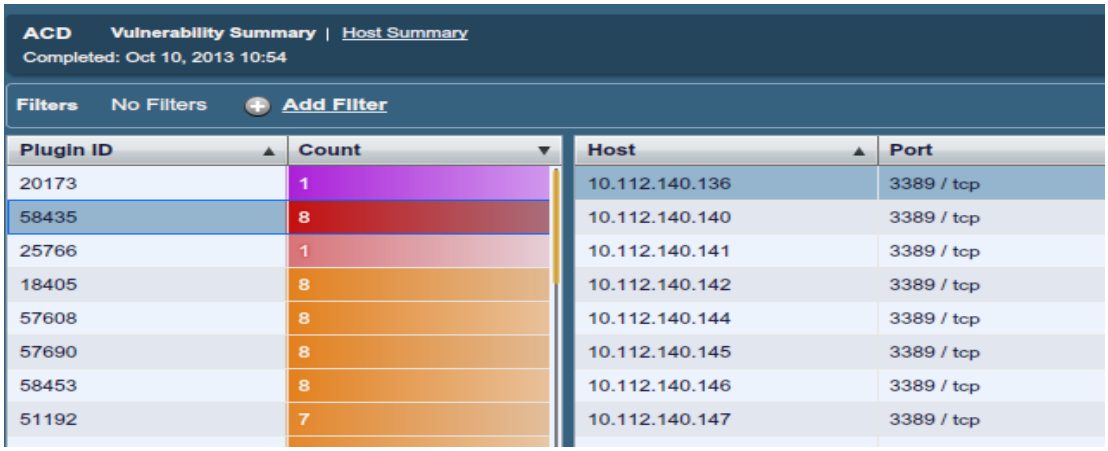



*Figura 16.* Análisis de vulnerabilidades de severidad alta
Fuente: Nessus
Elaborado por: William Chacón

Como se puede visualizar en la figura 16, 8 IP´s del equipo de Call Tacker tienen vulnerabilidad con severidad alta en el puerto 3389 de acuerdo a la lista de colores antes señalada. De acuerdo a lo analizado, este puerto permite enviar y recibir datos a través de los protocolos de trasmisión y datagramas de usuario utilizados para comunicarse mediante conexión de escritorio remoto, es decir, un intruso podría aprovechar esta vulnerabilidad para provocar que el sistema pueda ejecutar código arbitrario mediante el envío de secuencia de paquetes RDP (Remote Desktop Protocol).

Para poder prevenir este tipo de vulnerabilidades y ejecutar una denegación de servicio se deberá tener activo Windows Firewall para dejar los puertos deshabilitados en el caso de ser necesario para reducir el riesgo de los ataques.

- **Severidad Media**

  En este escenario se presenta las vulnerabilidades detectadas como severidad media marcadas con el color naranja, se pudo observar que varias IP`s tienen el puerto 3389 TCP (Transmission Control Protocol) abierto, es decir, son propensas a ataques realizando modificaciones, inserciones en los mensajes

incluyendo las credenciales de autenticación ente dos partes sin darse cuenta que el enlace de comunicación ha sido violado o alterado.

Severidad Media

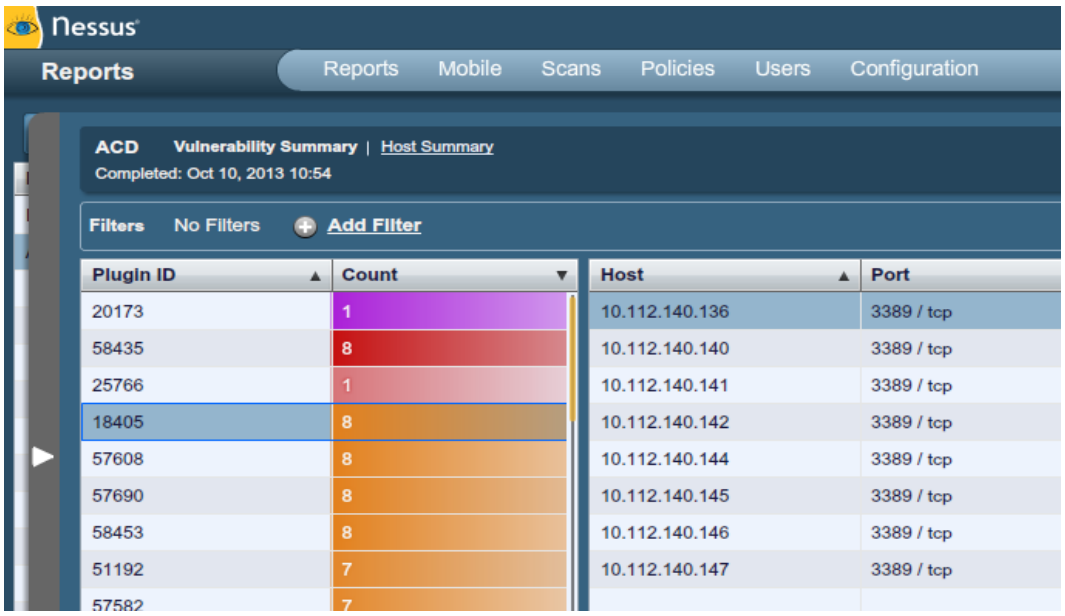



*Figura 17.* Reporte de vulnerabilidades severidad media
Fuente: Nessus
Elaborado por: William Chacón

Una de las posibles soluciones para prevenir es tener el uso de SSL que proporcionarán conexiones seguras por una red proporcionando cifrado de datos, autenticación de servidores, integridad de mensajes y autenticación de cliente para conexiones TCP/IP (Transmission Control Protocol / Internet Protocol).

También se consideró para el análisis las IP`s la lista de los siguientes equipos del equipo de Call Tacker:

10.112.140.136
10.112.140.141
10.112.140.142
10.112.140.144
10.112.140.145

En donde la herramienta nos emitió un reporte algunos inconvenientes relacionados con vulnerabilidades que se detalla a continuación:

Grupo de IP`s con severidad Media

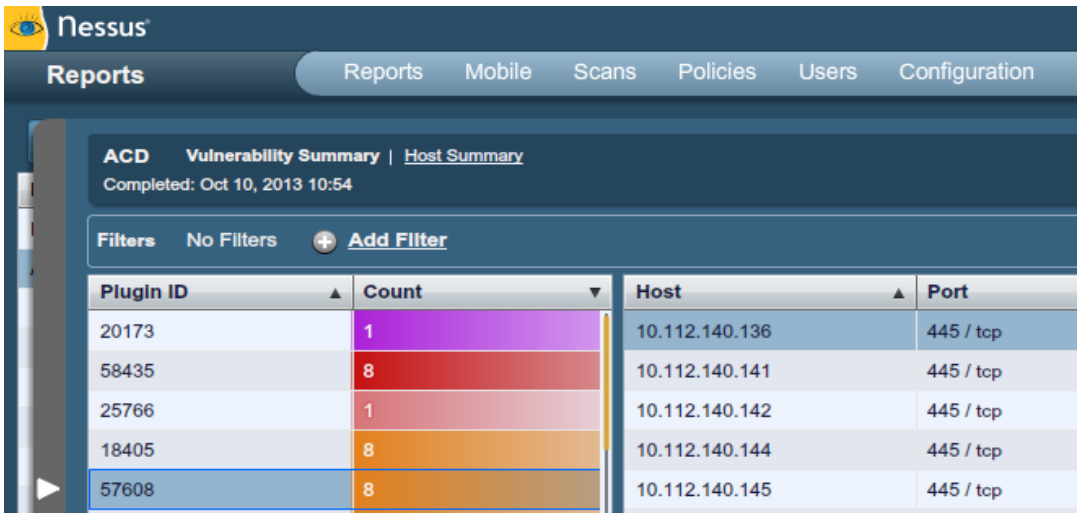



*Figura 18.* Reporte de vulnerabilidades de IP´s con severidad media
Fuente: Nessus
Elaborado por: William Chacón

Las condiciones expuestas en el informe, permiten realizar el análisis y determinar que si tenemos el puerto abierto 445 TCP pudiese permitir ataques man-in-the-midle contra el servidor SMB (Protocolo de intercambio de archivos), para poder mitigar este inconveniente se deberá exigir la firma de mensajes en la configuración del host, en el sistema operativo Windows este se encuentra en la directiva de seguridad local.

### 2.4.2. Servidor de CCpulse

Uno de los servidores más críticos es el CCpulse debido a que si se tiene algún inconveniente a este equipo no permitirá verificar los niveles de servicio que se brinda en ese instante.

Se realiza la exploración de los puertos abiertos se encontró las siguientes novedades:

Análisis CC Pulse

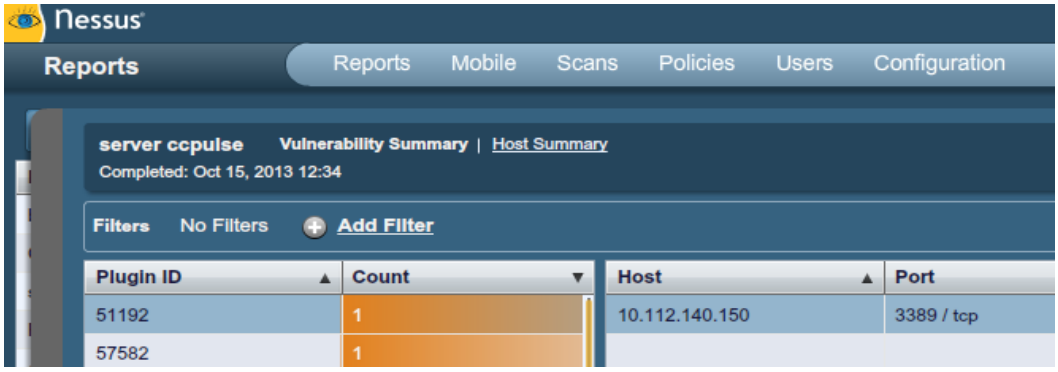



*Figura 19.* Análisis de vulnerabilidades del servidor de CCPulse
Fuente: Nessus
Elaborado por: William Chacón

La vulnerabilidad mostrada indica que no debe tener confianza en el certificado SSL (protocolo de seguridad que hace que los datos viajen de manera segura por internet), el certificado del servidor X.509 (Estándar para infraestructura de claves públicas) no tiene la firma de una autoridad de certificación pública conocida, esta situación puede presentarse en formas diferentes en la cual los certificados no se pueden confiar.

### 2.4.3. DNS (Sistema de nombres de Dominio) de Telefónica

Para poder brindar un valor agregado al cliente y evitar inconvenientes de acceso a información confidencial que puede ser manipulada para cometer ataques delictivos, se realizó un análisis de los DNS del cliente, la primera IP analizada es la 10.112.157.48 que se detalla los resultados a continuación:

Análisis severidad crítica DNS Telefónica

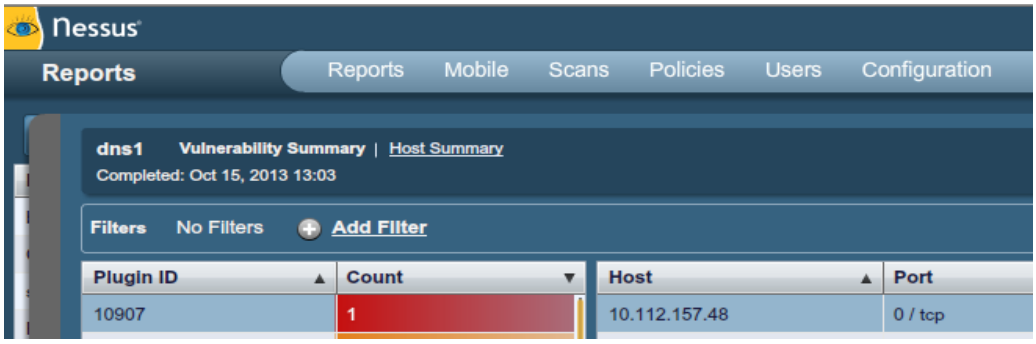



*Figura 20*. Análisis de severidad crítica del DNS cliente telefónica
Fuente: Nessus
Elaborado por: William Chacón

La cuenta "Invitados" tiene demasiados privilegios, usando las credenciales es posible determinar que pertenece a grupos distintos de huéspedes, los usuarios invitados no deben tener ningún privilegio adicional, para ello se determina restringir la pertenencia al grupo de la cuenta invitado.

Análisis severidad media DNS Telefónica

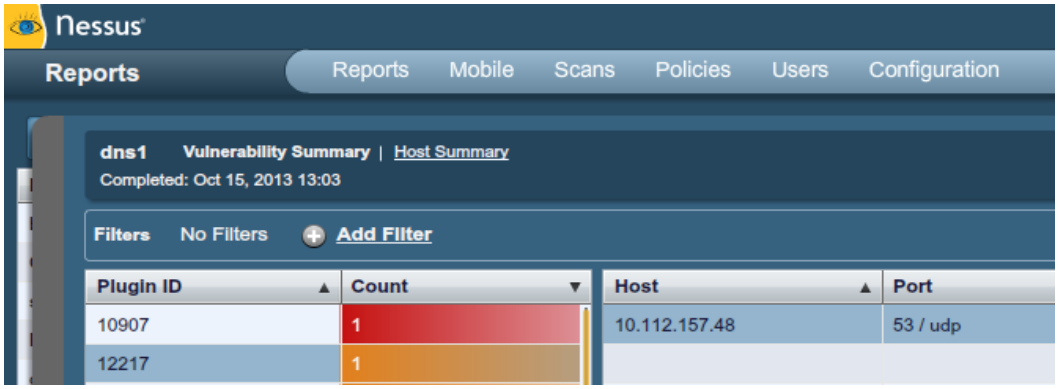



*Figura 21*. Análisis de vulnerabilidades de severidad media DNS Telefónica
Fuente: Nessus
Elaborado por: William Chacón

Otra de las vulnerabilidades es de severidad media verificando que hay un puerto abierto que es el 53 UDP (Protocolo de datagrama de usuario), el cual puede permitir ataques de espionaje caché permitiendo a un atacante remoto determinar que dominios recientemente se han resuelto a través de este servidor de nombres, si es un servidor DNS interno no es accesible a una red externa, los ataques simplemente se limitan en la red interna, esto puede incluir a los empleados, consultores, y los usuarios de una red de invitados o conexión WIFI.

### 2.4.4. Escaneo de puertos mediante NMAP

Se realiza el escaneo de cada una de las IP´s con la herramienta Nmap con la finalidad de conocer la topología y la estructura de cada uno de los equipos analizados mediante Nessus.

Escaneo de IPs mediante NMAP

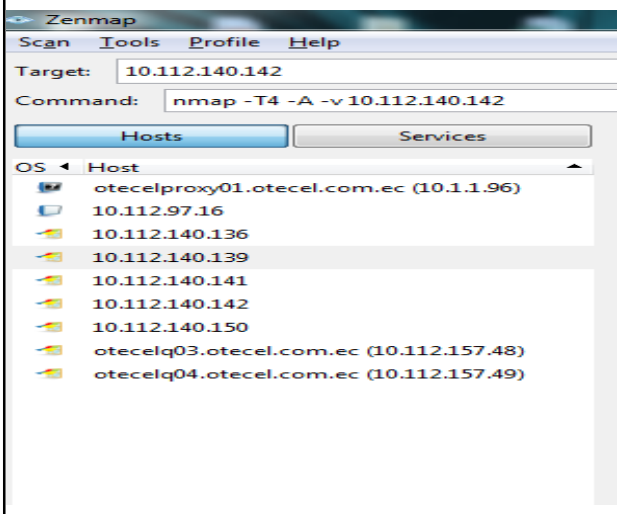



*Figura 22.* Escaneo de IP´s con la herramienta NMAP
Fuente: Nmap
Elaborado por: William Chacón

Topología mediante NMAP

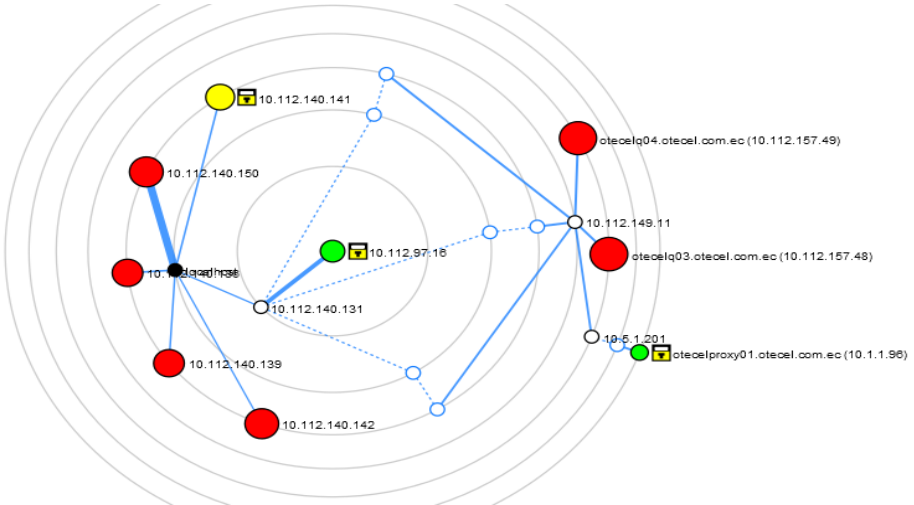



*Figura 23.* Topología y reporte de las Ip´s usando NMAP
Fuente: Nmap
Elaborado por: William Chacón

### 2.4.5. Análisis de vulnerabilidades mediante herramienta Conan

Para realizar el escaneo de vulnerabilidades se utilizará la herramienta Conan (Inteco Cert) con el fin de obtener información de las vulnerabilidades del sistema Operativo.

Para el caso de estudio se considera el seguimiento en el servidor de archivos.

Informe de análisis Conan


*Figura 24.* Reporte del análisis de Conan
Fuente: (Inteco, 2011)
Elaborado por: William Chacón

Una vez realizado el análisis, la herramienta nos dará a conocer la situación actual del servidor. Este informe está estructurado por dos partes:

- Datos Generales del Incidente detectado.
- Informe y Resumen del Análisis.

Mediante lo mencionado anteriormente se procede a describir la información en las siguientes figuras:

Análisis de la configuración del sistema

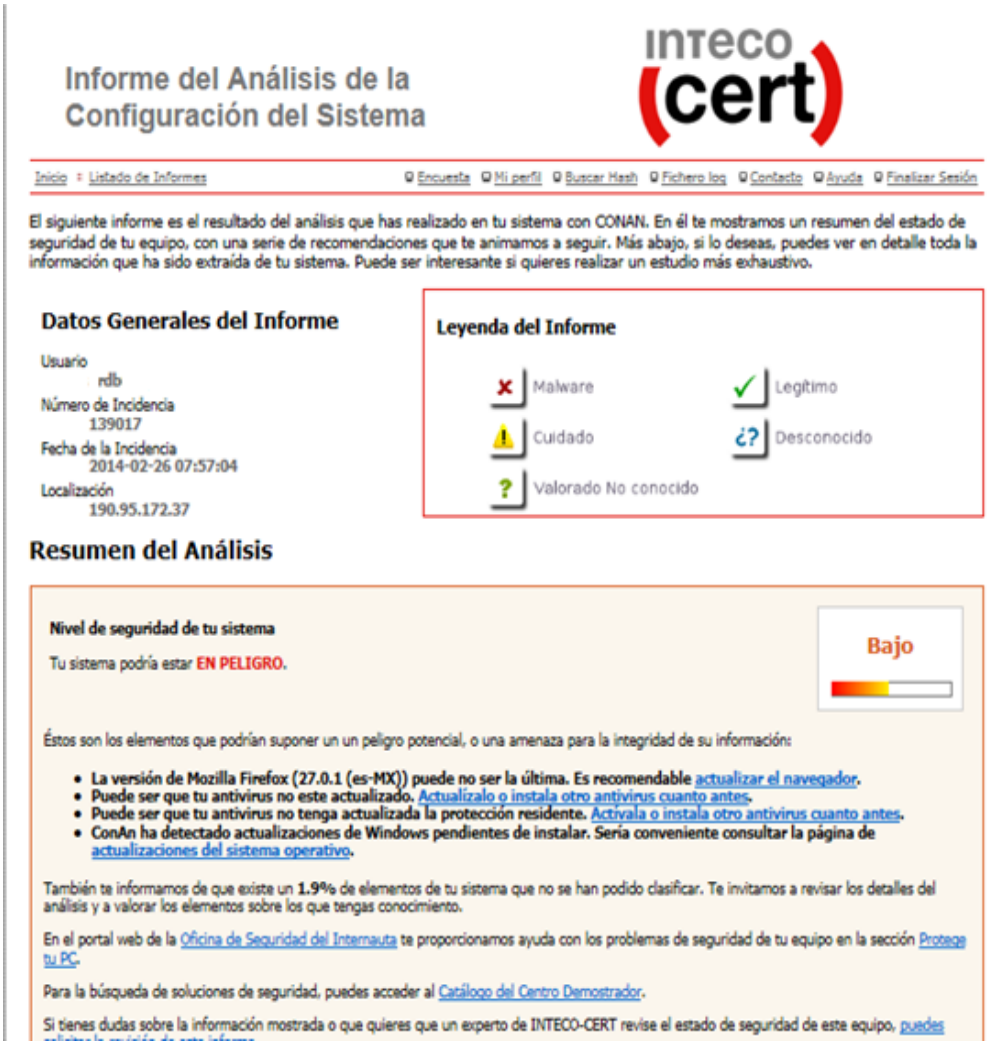



*Figura 25.* Reporte de vulnerabilidades encontrada en el servidor de archivos
Fuente: (Inteco, 2011)
Elaborado por: William Chacón

Como se puede observar en la figura 25, se tiene un resumen del análisis del servidor de archivos que se detalla a continuación:

2. Desactualización del navegador Mozilla Firefox.
3. Antivirus desactualizado.
4. Conan detecto actualizaciones pendientes de instalar.
5. Documentos sin clasificar.

A continuación se detalla la información detallada del servidor de archivos:

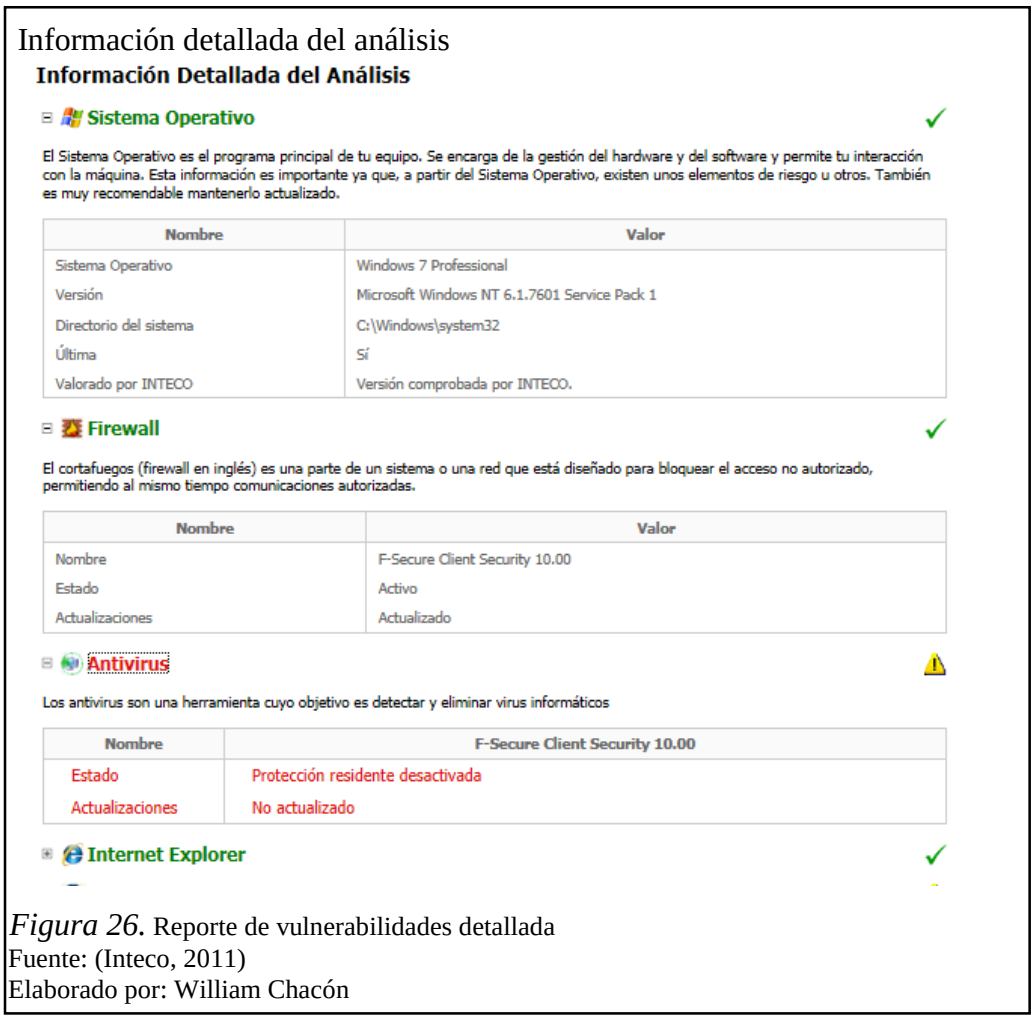



*Figura 26.* Reporte de vulnerabilidades detallada
Fuente: (Inteco, 2011)
Elaborado por: William Chacón

El informe muestra las recomendaciones y lineamientos que permiten al administrador del servidor tomar los correctivos necesarios para solventar los inconvenientes que puedan presentarse en el equipo.

En el caso puntual de estas recomendaciones se observa que el antivirus presenta alguna anomalía y este deber ser revisado y quizás la revisión del equipo con otra alternativa de antivirus.

## 2.5. Resultados obtenidos de la pruebas realizadas

Mediante los marcos de referencia expuestos anteriormente se realizó el análisis de la situación actual de Service Desk, manteniendo varios resultados de las pruebas realizadas en: Red interna, instalaciones, procedimientos, personal, a continuación se detallará las observaciones detectadas:

### 2.5.1. Red interna del Service Desk TELEFÓNICA – TCS

1. Falta de controles de seguridad de la información.

2. Desde el inicio del proyecto hasta la fecha no se ha realizado un análisis de vulnerabilidades.

3. Telefónica no ha entregado documentación con respecto a la seguridad de la información que se debe tener en el servicio.

    - TCS no cuenta con documentación con respecto a la seguridad de información que se debe tener en el servicio con Telefónica.

4. Las seguridades aplicadas a la red interna son básicas, solo cumplen con parte del Hardening de seguridad.

    - Todo proyecto puesto en producción debe constar con la certificación de seguridad el Service Desk, no ha sido certificado.

    - Dentro de la red del Service Desk se ha incluido más proyectos por lo que se han realizado excepciones a procedimientos sin conocimiento de Seguridad Informática.

5. A nivel de administración de la red se desconoce procedimientos para la configuración y monitoreo de la red.

6. El registro de acciones se mantiene en logs de configuración de equipos, que cuando se configuran nuevamente se borra el anterior por lo que hay logs históricos.

### 2.5.2. Instalaciones Service Desk TELEFÓNICA – TCS

1. Para el ingreso y acceso al cuarto de equipos no se mantiene un proceso de seguridad implementado.

2. No se cuenta con redundancia de energía eléctrica.

3. Desorden en el cuarto de equipos.

### 2.5.3. Procedimientos Service Desk TELEFÓNICA – TCS

1. No existe documentación alineada al cumplimiento del servicio y objetivos de TI.

2. La información existente no ha sido difundida entre todo el personal.

3. No existe una clasificación de información difundida ni aplicable a la documentación existente.

    - No se cuenta con procedimientos entregados por el cliente.

### 2.5.4. Personal Service Desk TELEFÓNICA – TCS

1. Procedimientos de servicio no formalizados.

2. Desconocimiento de procedimientos de servicio existentes.

3. Falta de difusión de procedimientos.

# CAPÍTULO 3

# MECANISMOS DE PREVENCIÓN

## 3.1. Organización del proyecto

Una vez realizado el levantamiento de información se han identificado criterios negativos en el Service Desk, es así cada uno de los puntos se encuentran descritos en el anexo #9. Para la elaboración de las medidas de prevención que el Service Desk debería ejecutar para evitar problemas a futuro, se debe realizar un Input de información, que en este caso será el análisis de los puntos encontrados en el anexo #9.

El total de problemas y/o vulnerabilidades detectadas en función a la situación actual son un total de 15, que están distribuidas por: Infraestructura (Red interna), instalaciones, procedimientos, personal por lo que se ha definido realizar un análisis previo por cada criterio de investigación.

### Infraestructura (Red interna)

Para la revisión de la red interna correspondiente al Service Desk Telefónica-TCS se utilizó marcos de referencia de ISO 27002 e informática forense, la información proporcionada por la administradora de la red y seguridad informática ha sido de gran utilidad para conocer las debilidades que tiene el servicio, es decir posibles filtraciones de información que pueden causar pérdidas económicas a la empresa.

No se tiene información o documentación proporcionada por el cliente que indique sobre el manejo de su información por categorías de criticidad y que sean difundidas al personal del Service Desk para su cumplimiento, lo único que se tiene firmado es un contrato de confidencialidad de la información a nivel general.

No se realiza un análisis de vulnerabilidades periódicas y puertos abiertos, por lo tanto las mismas con el pasar del tiempo pueden convertirse en problemas causando afectación a la comunicación entre cliente - proveedor, acceso a las aplicaciones, bases de datos u otros. Adicional no se tiene un sistema de detección de intrusos (IDS) que permita detectar actividades sospechosas o accesos no autorizados por el personal.

No se ha trabajado conjuntamente con seguridad informática para mejorar y establecer controles en la red interna, en este momento solo se encuentra puesto en operación el Hardening interno de TCS, para nuestra revisión se ha utilizado herramientas de investigación de informática forense, detectando lo siguiente:

- Se identificaron Puertos de conexión abiertos.
- Equipos de ingenieros de soporte con permiso de administrador.
- Desbordamiento de Búfer.
- Estaciones de trabajo con navegadores desactualizados.
- Antivirus desactualizado.
- Actualizaciones pendientes de instalar.
- Documentos sin clasificar.

Con lo cual la red está propensa ataques internos. Adicional se ha identificado que no se ha realizado un análisis de vulnerabilidades a la red interna desde su puesta en producción, ni se ha realizado actualizaciones o tomado respaldos de información, esto se ha dado debido a que los proyectos han salido a producción en tiempos record sin mayor revisión.

Los errores y criterios negativos encontrados no pueden ser considerados como riesgo crítico sino más bien riesgo moderado debido a que el proyecto es pequeño sin embargo se debe tomar los correctivos necesarios para evitar pérdidas de continuidad en el servicio que terminarían en sanciones por parte del cliente.

**Instalaciones del Service Desk**

Para la revisión de las instalaciones correspondientes al cuarto de equipos del Service Desk Telefónica – TCS se utilizó uno de los marcos de referencia de ISO 27002, la toma de información y captura de evidencias se realizó mediante Check List y observación directa.

Bajo estas características se han identificado 3 criterios que podrían llegar a ser un problema o en su momento provocaron una pérdida en la continuidad del servicio.

Dentro del marco de referencia escogido para las instalaciones podemos interpretar de su teoría lo siguiente:

Toda instalación en la que se encuentre equipos de comunicación o encargados de la transmisión de información debe contar con seguridades físicas establecidas, controles de acceso, redundancia en el funcionamiento para evitar pérdidas de continuidad, y un orden en la distribución de cables, para todo lo normado dentro de un marco de referencia se tiene conocidas buenas prácticas que permiten cumplir con las seguridades, orden y redundancia que es lo más fuerte con lo que debería contar un cuarto de equipos, claro que cada uno de estos puntos debe ser analizado para el tamaño de cuarto de equipos y por el servicio que oferta y la funcionalidad que cumple.

El cuarto de equipos no solo brinda servicio de comunicación y trasmisión de datos al Service Desk si no que cuenta con 4 servicios adicionales, es por eso que se debe mantener un orden en el cableado y una redundancia inmediata que permita la continuidad del servicio ofertado que es 24 x 7.

En el Service Desk la redundancia es considerada como un tema crítico debido a solicitud del cliente por el servicio ofertado 24 x 7. De la revisión realizada se identificó que no se cuenta con redundancia en la conexión eléctrica, siendo vulnerable a la continuidad del servicio ya que los ups existentes tienen tiempo máximo de duración de dos horas, y así incurrir en multas elevadas a la facturación de TCS significando pérdidas económicas e inconformidad del servicio brindado.

El ingreso a las instalaciones del edificio Pucará cuenta con las seguridades del edificio en la puerta principal de la planta baja siendo accedidas con tarjetas magnéticas, sin embargo en el piso 1 es de libre acceso a cada uno de los proyectos y en el caso de ser una persona externa se mantiene un registro manual. Se cuenta con cámaras de seguridad pero como se indicó anteriormente el cuarto de equipos no se encuentra aislado sino en las oficinas más grandes sin mantener ninguna restricción ni seguridad, es por eso que el personal tiene acceso libre a la revisión y manipulación dentro del cuarto de equipos. Este inconveniente podría ocasionar intencionalmente la afectación a cada uno de los servicios, desconectando algunos de los ups y este dejando sin las 2 horas de funcionalidad a los equipos en caso de

fallas eléctricas, o la posible manipulación de cableado provocando desconexiones en los servicios.

El tamaño del cuarto de equipos no es complementario para mantener un orden en el cableado que permita identificar la red y la conexión correcta; de las revisiones realizadas se puede observar que los equipos y cableado no cuentan con un etiquetado o algún otro tipo de identificación que permita al administrador a cargo o personal que ingrese al cuarto de equipos conocer el segmente de red, proyecto o tipo de conexión a la que pertenece, es considerado un riesgo crítico tomando en cuenta que no se tiene medidas de acceso ni un orden específico.

**Madurez de procedimientos en el Service Desk**

Al inicio de la presente tesis se definió como uno de los marcos de referencia para la revisión de la normativa de COBIT, dentro de su marco teórico está normativa ha definido una matriz de madurez en procedimientos, en función del tipo y cantidad de documentación que tiene una empresa independientemente que sea: Privada, pública, grande, mediana, pequeña.

Partiendo de este marco de referencia se realizó una revisión minuciosa de la información que mantiene actualmente el proyecto, tomando en cuenta la documentación entregada por parte del cliente como dueño del servicio y la documentación del proyecto generada por el proveedor en este caso TCS.

Según lo definido anteriormente podemos definir que el proyecto Service Desk de Telefónica se encuentra en un nivel de madurez 2, es un nivel Repetible ya que muchos de los procesos son utilizados tanto por el área de ACD como el área de aplicaciones, además no se cuenta con la comunicación formal y entrenamiento al personal sobre la documentación existente, esta calificación indica que la organización tiene riesgos latentes en su propio personal puesto que no se ha puesto en conocimiento de todos los procesos de la empresa y los errores se convierten en algo muy probable (Véase figura #4).

Para la revisión de los procedimientos nos apoyamos en herramientas de investigación como entrevistas, Check List teniendo el siguiente análisis:

- **No existe documentación alineada al cumplimiento del servicio y objetivos TI**

Este punto fue encontrado como falencia debido a que se revisó la documentación que existe y se revisó que contienen, su presentación e involucrados, es decir que objetivos abarca y a quienes va dirigido.

De la revisión se puede ver que la poca documentación que existe del proveedor no se encuentra alineada al servicio ya que la mayoría de información está orientada a los servicios que más abarca TCS que son los servicios a entidades bancarias. Perjudicando a la entrega de servicio a entidades como Telefónica que nada tienen que ver con la Banca. En función de esto el personal de cada área ha ido definiendo documentación fuera de estándar y no aprobada por la gerencia para poder entregar el servicio. Cuando la documentación propia del proveedor no está orientada a los objetivos del servicio sin tener lineamientos de entrega del servicio poniendo en peligro la continuidad con el cliente.

- **La información existente no ha sido difundida entre todo el personal**

Del Check List realizado al personal del Service Desk se puede evidenciar que el personal desconoce de documentación existente para la entrega de servicio al cliente. Todo servicio debe contar con lineamientos claros para la entrega de un buen servicio, si el personal desconoce de la documentación de apoyo existente puede retrasar la entrega del servicio.

El Service Desk cuenta con documentación para la entrega del servicio según el área pero esta documentación se encuentra disponible en un compartido pero al personal sobre todo al nuevo, no se le ha indicado que contiene cada documento.

La falta de distribución de información y documentación puede provocar fallas en el cumplimiento de niveles al ser un proyecto con alto grado de rotación de personal debería mantener todo el tiempo un plan de difusión o comunicación de la existencia de la documentación que aunque no está aprobada por la gerencia es de gran apoyo en la entrega del servicio.

- **No existe una clasificación de información difundida ni aplicable a la documentación existente**

El Service Desk manipula información que debería ser tratada como confidencial, interna y sensible.

De las revisiones realizadas podemos identificar que no se ha realizado una clasificación de información, es decir el personal que manipula la información desconoce si la información con la que está trabajando es confidencial, sensible, pública o si tiene algún grado de criticidad.

El personal no tiene conocimiento sobre el grado de importancia de la información que mantiene el cliente, es por eso que puede ser manejada, extraída, manipulada sin el más mínimo cuidado. Estas debilidades podrían causar pérdidas económicas directamente al cliente, por lo que es necesario que el personal este consiente de qué valor tiene la información con la que está trabajando.

- **No se cuenta con procedimientos entregados por el cliente**

Esta observación encontrada es considerada como baja ya que el cliente debería normar como desea recibir el servicio, bajo que lineamientos, pero no es obligación del cliente entregar políticas para que su proveedor las cumpla.

Por el tipo de servicio los procedimientos deberían ser labor directa de quien conoce y entrega el servicio que en este caso es TCS.

**Personal**

Por definición el personal fue revisado utilizando como referencia lo que nos norma ITIL, se utilizó entrevistas y observación directa del servicio para la toma de evidencias.

De esta revisión se ha encontrado aspectos que el personal ha indicado no conocer o que se observa falencias en los procesos de servicio. ITIL norma que los

procedimientos para entrega de servicios deben estar conocidos por el personal que entrega el servicio y que todo procedimiento debe estar formalizado para su uso. En función de esto tenemos:

- **Procedimientos de servicio no formalizados**

Este punto también fue analizado con la normativa de COBIT en su madurez de procedimientos y se lo vuelve a encontrar en la revisión realizada al personal mediante ITIL. El no tener procedimientos formalizados puede ocasionar responsabilidades mal dirigidas en caso de fallas en el servicio, ya que la gerencia desconoce documentación existente, en el caso del servicio ofertado se tiene documentación antigua desde el proveedor anterior esta documentación es de gran utilidad y ha sido desarrollada por los ingenieros de soporte a cargo de entregar el servicio por lo que los derechos de autor podría adquirirlos TCS, pero como ha existido poco interés por parte de los líderes de proyecto para conocer sobre la documentación esta sigue sin formalizarse.

- **Desconocimiento de procedimientos de servicio existentes**

Como se indicó en el punto anterior los líderes de proyecto del Service Desk se han despreocupado en gran parte de conocer la documentación existente por lo que no han exigido su difusión en el personal y asumen que la capacitación ira pasando de operador en operador. Tomando en cuenta que la rotación de personal es alta en el servicio se ha ido perdiendo conocimiento de documentación existente, porque existen manuales y procedimientos disponibles que ayudarían a agilizar la entrega de servicio o serian de gran apoyo en caso de desconocimiento sobre temas propios del cliente pero no están siendo utilizados por que no están formalizados ni son conocidos ocasionando doble esfuerzo en el personal ya que debe buscar soluciones a temas que ya están documentados.

- **Falta de difusión de procedimientos**

La falta de difusión en el personal es responsabilidad directa del coordinador a cargo de cada área, que al igual que los líderes de proyecto asume el conocimiento de la documentación por parte de los ingenieros de soporte.

El momento que se levanta nueva documentación se realiza la difusión se indica el path donde reposará y una explicación de su uso, pero existe información anterior que no se han preocupado por dar a conocer.

Durante las revisiones realizadas se puede observar manuales no formalizados pero que contienen procedimientos o problemas existentes en el cliente que han sido corregidos y probados. Por lo que al no saber su existencia exige al ingeniero de soporte nuevamente consultar e investigar una solución a algo que ya está definido.

## 3.2. Herramientas y metodologías de prevención

Como se apreció en la tabla #3 se tiene varias herramientas de informática forense para la prevención y detección de siniestro, en el caso de estudio de la presente tesis se definieron varias herramientas para el diseño de medidas preventivas que se detalla a continuación:

- Snort
- Hardening
- Fbackup

### 3.2.1. Plan de prevención

El plan de prevención es un documento formalizado que debe ser autorizado para la ejecución en una empresa. Recoge la normativa, reglamentación, y los procedimientos, definiendo los objetivos de prevención, responsabilidades, funciones a lo que se refiere infraestructura tecnológica, procedimientos, personal, instalaciones.

El plan de prevención que se elaborará en el siguiente capítulo es una recopilación de normas, procedimientos, políticas y recomendaciones con el fin de asegurar la prevención de riesgos teniendo en cuenta los objetivos planteados en el plan de medidas preventivas.

El pan de prevención debe contener la estructura organizativa, responsabilidades, procedimientos, procesos y recursos necesarios para llevar a cabo la política de prevención en el Service Desk.

Según lo explicado, de nuestra revisión se ha definido que la presentación de medidas preventivas se realice utilizando planes de prevención, que permitan entregar dichas medidas documentadas y listas para ser analizadas y ejecutadas, en función de esto los planes de prevención estarán regidos bajo el siguiente esquema:

**Plan de prevención**

- Objetivos
- Alcance
- Antecedentes
- Involucrados
- Descripción del trabajo
- Condiciones de implementación
- Conclusiones

Los planes deberán ser documentados de tal manera que sean fáciles de entender y contengan criterios de tecnología, seguridad y continuidad de los servicios. Todo este esquema además tendrá definiciones apoyadas especialmente en la informática forense.

### 3.3. Mecanismos de prevención aplicables a la mesa de ayuda

Mediante el uso de marcos de referencia basados en auditoría de sistemas para seguridad de la información, informática forense y la aplicación de herramientas para la obtención de información del proyecto Service Desk de Telefónica se realiza el análisis de la situación actual de la Mesa de Ayuda enfocado en aspectos de: red interna, instalaciones, procedimientos y personal, de este análisis se pudo constatar que el servicio se encuentra expuesto a riesgos con diferentes categorías de severidad: crítico, medio y bajo, existen riesgos categorizados como críticos sin embargo por el tamaño del proyecto bajan la categorización de critico a bajo o medio.

Por el tamaño de proyecto, muchos de los controles de seguridad deben ser analizados, la necesidad de colocarlos, el costo al tenerlos y si la inversión que se realizaría para colocarlos tal cual mandan los marcos de referencia son aplicables al proyecto, tomando en cuenta lo descrito se ha podido unificar riesgos para diseñar propuestas de resolución y recomendaciones sobre cómo se podría mitigar las vulnerabilidades identificadas, las propuestas emitidas primero han sido definidas en función de lo normado por la informática forense y tomando en cuenta la magnitud de costos y dificultad en su aplicación. El proyecto por ser un proyecto pequeño no debe incurrir en demasiados costos, tiempo y esfuerzo para la implementación de controles de seguridad.

Tomando en cuenta la información que transmite el proveedor es crítica, deberá implementar controles acorde a su disponibilidad de costos y tiempo. En función de esto se definieron 6 medidas de prevención de implementación media y costos bajos, las mismas que a continuación serán descritas.

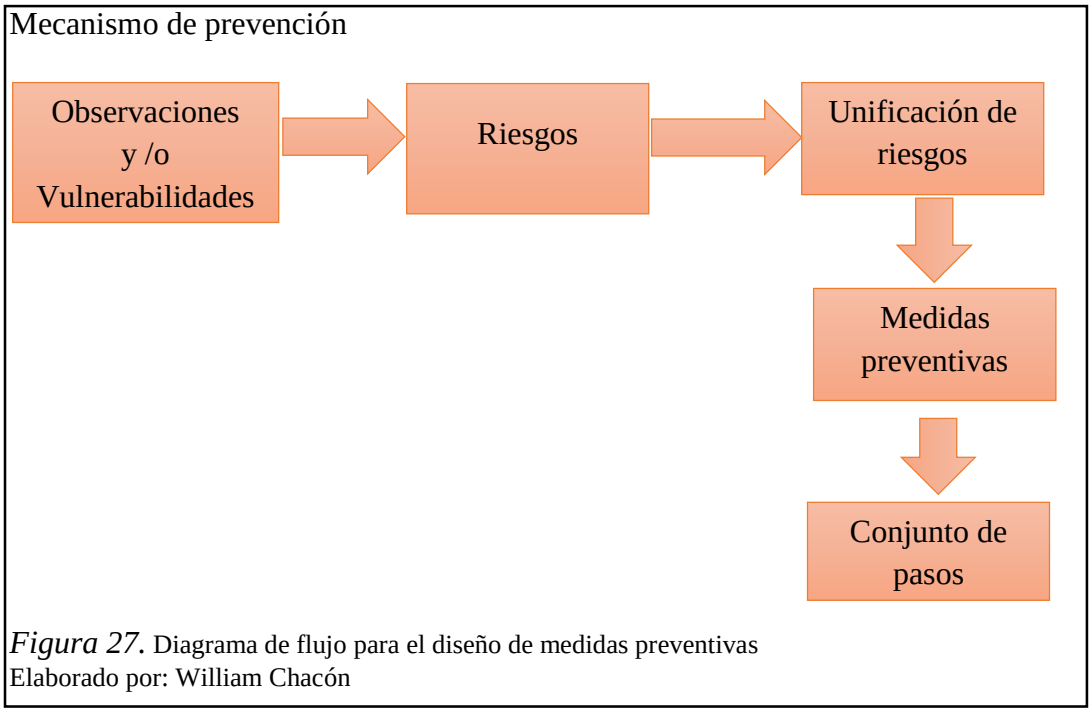



*Figura 27.* Diagrama de flujo para el diseño de medidas preventivas
Elaborado por: William Chacón

### 3.3.1. Análisis F.O.D.A.

El proyecto Service Desk de Telefónica tiene funcionalidad de 2 años, durante este tiempo se ha podido definir un FODA, este ha sido de gran ayuda en la resolución de la presente tesis. En el estado actual este sería el escenario.

Tabla 9. *Análisis F.O.D.A.*

| **Fortalezas** | **Oportunidades** |
|---|---|
| * Personal antiguo en cada uno de los servicios dando soporte dentro de las áreas.<br><br>* Ambiente de trabajo favorable y amistoso entre las áreas.<br><br>* TCS como empresa multinacional prepara a sus colaboradores periódicamente en distintos temas. | * Evaluación periódica del cliente al servicio.<br><br>* Telefónica puede incrementar más servicios a cargo de TCS.<br><br>* Apoyo del cliente en caso de inconvenientes con el servicio. |
| **Debilidades** | **Amenazas** |
| * Inexistencia de documentación que norme el servicio.<br><br>* Conocimiento del personal antiguo no difundido a los nuevos colaboradores.<br><br>* Capacitaciones al personal sin un procedimiento definido a seguir.<br><br>* Proyecto en producción sin certificación.<br><br>* Personal nuevo no conoce al 100% las políticas internas y los procesos del cliente. | * Desconocimiento de vulnerabilidades existentes del cliente<br><br>* Desconocimiento de procesos de configuración de equipos del cliente.<br><br>* Definición de multas económicas por contrato al incumplimiento del servicio.<br><br>* Desconocimiento del servicio por parte de Telefónica. |

Nota. Análisis F.O.D.A
Elaborado por: William Chacón.

Las fortalezas y oportunidades han sido la base del servicio actualmente, estas han permitido la continuidad y en cierta parte han evitado que el cliente aplique sanciones de ámbito económico al proyecto.

Las debilidades y amenazas pese a que aún no se han presentado son un riesgo latente al servicio, de no corregirlas a tiempo podrían ocasionar la pérdida del contrato o incumplimiento al mismo, trayendo como consecuencia multas económicas o problemas legales por incumplimiento.

Con el estudio realizado en la presente tesis lo que se ha conseguido es emitir medias preventivas que mitiguen las debilidades y amenazas existentes dando mayor fortaleza y fundamento a las fortalezas y oportunidades del servicio.

La implementación de manera eficaz de las medias preventivas hará que el servicio mejore su calificación y suba en su calidad, haciendo que el cliente reconozca el plus entregado por la empresa TCS, y de tal manera que el cliente se interese en poner a cargo de TCS más proyectos de tecnología, confiando en que siempre recibirá algo adicional siempre con miras a mejorar.

### 3.4. Diseño de medidas preventivas de seguridad informática

A continuación se detallará el diseño de medidas preventivas que constan de 3 partes: Evaluación, identificación, plan de prevención. Las mismas deberán ser aplicables al servicio de mesa de ayuda:

**Objetivos**

- Brindar una mirada introductoria y metodológica de la informática forense como herramienta de prevención para combatir la ciber delincuencia, mediante un plan de prevención para el proyecto Service Desk de Telefónica en los marcos de infraestructura red interna, procedimientos, instalaciones y personal que enfrenten una vulnerabilidad detectada en sus operaciones y que puedan ser de impacto al servicio.

**Alcance**

El presente documento está basado en una metodología de informática forense, que permite usar definiciones de informática forense para prevención y será aplicable al proyecto Service Desk de Telefónica en los ámbitos de infraestructura red interna, procedimientos, instalaciones y personal que desempeña el servicio.

**Antecedentes**

Se ha realizado un análisis de situación actual del proyecto mediante la aplicación de técnicas científicas y analíticas especializadas a la infraestructura tecnológica que

permite identificar, preservar, analizar y presentar datos que sean válidos y puedan ser utilizados para tomar medidas preventivas que eviten la presencia de riesgos a la seguridad de la información.

Como indica la teoría de la informática forense, se realizó la recolección de evidencias mediante marcos de referencia y herramientas de investigación escogidos según los expertos y criterio del investigador, de esa evidencia se han realizado el análisis y se han definido medias preventivas que más adelante serán detalladas.

**Las medidas preventivas definidas**

Las medidas preventivas que a continuación serán definidas, son el resultado del análisis realizado a la situación actual del proyecto Service Desk de Telefónica.

**Red interna**

- El proyecto Service Desk de Telefónica debe obtener la certificación de Seguridad emitida por el área de Seguridad Informática TCS.

- Revisar los procesos de monitoreo y administración aplicados al proyecto Service Desk de Telefónica.

**Instalaciones**

- Definir la ubicación del cuarto de equipos.

- Implementación de controles de seguridad en cuarto de equipos.

**Madurez en los procesos**

- Revisión a los procedimientos necesarios para el proyecto Service Desk de Telefónica.

**Personal**

- Realizar una capacitación al personal.

**Involucrados**

- **Área de Seguridad Informática TCS:** ayuda a mejorar la protección del hardware y software para brindar el servicio.

- **Administrador de red:** es la persona involucrada en el correcto funcionamiento de la red y la comunicación con el cliente Telefónica.

- **Gerencia del proyecto:** es la responsable del correcto funcionamiento del proyecto y la satisfacción del cliente con el servicio entregado.

- **Personal del Service Desk:** personal involucrado en operar el servicio.

- **Personal administrativo:** personal de mobiliario de los activos del proyecto.

- **Proveedor TE UNO:** Proveedor que brinda monitoreo de la red del proyecto.

- **Contraparte de Telefónica:** Cliente que solicita el servicio.

**Descripción del trabajo**

A continuación se describe la forma de implementación de las medidas preventivas, su implementación será tomando en cuenta los elementos existentes y la posibilidad de uso, así como costo - beneficio de las mismas sobre el proyecto Service Desk.

**Red interna**

1. Aplicar el Hardening propuesto por el área de Seguridad Informática con sus respectivos controles al proyecto Service Desk para obtener la certificación de seguridad, definir una periodicidad para el análisis de vulnerabilidades por parte de TCS y acordando revisiones por parte del cliente, esto con el fin de colocar controles que eviten ataques a la red interna que puedan concluir con el robo de información o perdidas de conexión perjudicando a la continuidad del servicio desatando un delito informático o multas económicas por parte del cliente.

**Probabilidad de riesgo al no aplicar la medida preventiva**

Red insegura cliente – proveedor, tendiente a ataques que provoquen caídas en el servicio, robo de información, indisponibilidad de aplicaciones. Poniendo en riesgo la integridad, confidencialidad, disponibilidad de la información utilizada en dar el servicio.

Acceso a la información crítica y confidencial realizando cambios internos sin autorización, permisos de administración, accesos no autorizados. Cualquiera de estos inconvenientes podría desatar un delito informático, esto puesto que lo más importante en la actualidad es el activo de información la cual en esta observación se encuentra en riesgo.

**Cumplimiento a la medida preventiva**

- Coordinar con el área de seguridad informática TCS la autorización para comenzar con la implementación del Hardening y tiempos de duración de la implementación del mismo sobre el proyecto para la obtención de la certificación de seguridad.

- Coordinar con el área de seguridad informática la elaboración de procedimientos de seguridad específicos como administración de usuarios y políticas de configuración de red para la infraestructura y aplicaciones del Service Desk con la ayuda y colaboración del personal interno más antiguo del proyecto.

- Realizar un proceso sistemático que permita conocer la identificación de debilidades y vulnerabilidades dentro del proyecto.

- Definir tiempos específicos para la ejecución del Hardening que permitirá la certificación del proyecto por parte del área de Seguridad informática.

- Implementar una herramienta para la detección de vulnerabilidades.

- Mantener una bitácora de los logs ejecutados del IDS (Sistema de detección de intrusos)

**Recomendaciones luego de aplicar la medida preventiva**

- Realizar el seguimiento oportuno de las vulnerabilidades encontradas dando cierre a las mismas mediante la implementación de controles o cambios en la configuración de la red.

- Realizar un análisis de costo beneficio que permita conocer la factibilidad de implementar un IPS y un IDS según lo expuesto en la propuesta de resolución, o por lo menos definir la implementación de uno de los 2.

- Realizar un seguimiento y ejecución del Hardening cada 3 meses.

- Para realizar el análisis de vulnerabilidades se puede usar Nessus como herramienta complementaria a MBSA (Microsoft Baseline Security Analyzer)

- Medir la situación actual del servicio referente a la detección de vulnerabilidades cada 6 meses y conocer si se redujo el riesgo mediante la operación de la medida preventiva.

**Propuesta de contingencia**

La propuesta de contingencia hace mención de que pese a las medidas preventivas y controles colocados se presente el riesgo.

Los puntos a ejecutar son los siguientes:

- Identificar las debilidades y vulnerabilidades encontradas luego de ejecutar las medidas preventivas.

- Documentar las vulnerabilidades encontradas y definir los problemas que ocasionaron al no ser identificadas.

- Realizar un estudio profundo con el fin de conocer el riesgo conjuntamente con seguridad informática para su mitigación definitiva.

- Definir el plan de acción para la corrección de las vulnerabilidades y corrección de errores ocasionados por la falta de medidas de seguridad.

- Implementar nuevos pasos en el Hardening con el fin de mitigar las vulnerabilidades que ocasionaron un incidente o problema de seguridad.

**Involucrados**

- Área de Seguridad Informática TCS.
- Administradora de la red.
- Gerencia del proyecto.

2. Realizar una revisión a los procesos de monitoreo y administración que aplica TEUNO en el servicio que oferta a TCS y acordar la elaboración de una bitácora de logs o un histórico de configuraciones que permitan en caso de inconvenientes mantener pistas de auditoria que permitan la resolución de inconvenientes de manera rápida y eficaz.

**Probabilidad de riesgo al no aplicar la medida preventiva**

Falta de conocimiento de monitoreo, pistas de auditoria y logs que permitan identificar cambios históricos realizados en la configuración de los equipos, útiles en caso de inconvenientes o ataques que des configuren el software base y configuración actuales de los equipos.

**Cumplimiento a la medida preventiva**

- Revisar el procesos de monitoreo y administración de la red interna del proyecto.

- Elaborar un plan de capacitación con el fin de involucrar al administrador de red de TCS en el monitoreo de red del servicio de Service Desk.

- Realizar categorías de severidad (alta, media, baja) mediante límites definidos sobre las vulnerabilidades que pueden encontrarse en la operación del

servicio y brindar mejoras para reducir el riesgo que pueda presentarse en la red interna del servicio.

- Almacenamiento histórico de logs.

- Definir un proceso de revisión de logs.

**Recomendaciones luego de aplicar la medida preventiva**

- Realizar una reunión para la revisión de los procesos de monitoreo y administración conjuntamente con seguridad informática, proveedor TE UNO, administrador de red TCS y solicitar al personal asistente documentar las capacitaciones.

- La administración de red deberá trabajar conjuntamente con el proveedor TE UNO para la gestión y monitoreo de red interna del servicio de mesa de ayuda, con el fin de identificar a tiempo falencias en el monitoreo y correcciones inmediatas de errores frecuentes.

- Implementar un espacio en el servidor para el almacenamiento histórico de logs que permita identificar los cambios en los equipos, mismos que deberían ser revisados cada 3 meses por el administrador, realizando a la par una liberación del espacio.

- Trabajar en equipo proveedor – administrador de red, con el fin de obtener el mismo conocimiento y poder actuar de manera eficiente ante los posibles problemas de la red interna.

**Propuesta de contingencia**

Si a pesar de aplicar la medida preventiva no se tiene resultados se recomienda los siguientes pasos:

- Revisar el error producido y su afectación al servicio.

- Determinar existencia de documentación para el error producido y definir responsables de la validación.

- Definir nuevamente un plan de capacitación con seguridad informática, proveedor TE UNO, administrador de red con el fin de reforzar el conocimiento adquirido en los pasos de la medida preventiva.

- Trabajar conjuntamente con el proveedor TE UNO y administración de red con el fin de mitigar por completo errores futuros sobre el mismo tema.

**Involucrados**

- Área de Seguridad Informática TCS.
- Administradora de la red.
- Gerencia del proyecto.
- Proveedor TE UNO

**Instalaciones**

1. Definir la ubicación del cuarto de equipos fuera de una de las oficinas y definir un control de acceso más fortalecido que la bitácora manual que actualmente aplican.

**Probabilidad de riesgo al no aplicar la medida preventiva**

Personal no autorizado accede al cuarto de equipos y podría realizar cambios innecesarios e intencionales en la red interna del Service Desk, desconexión de cables en el switch, desorden de los equipos, etc. Afectando de esta manera la continuidad del servicio, pudiendo perder paquetes que se estén enviando o receptando, demora en la entrega de información al cliente, sanciones por interrupciones del servicio.

**Cumplimiento a la medida preventiva**

- Cambio de ubicación del cuarto de equipos del proyecto.

- Mejorar los controles de seguridad en el área del cuarto de equipos, mantener supervisión de las personas que realizan cualquier actividad dentro de la misma.

- Registrar el acceso al cuarto de equipos.

- Realizar revisiones periódicas para localizar a tiempo dispositivos de grabación no-autorizados, armas con el fin de evitar el acceso al cuarto de equipos.

**Recomendaciones luego de aplicar la medida preventiva**

- Mantener una reunión con gerencia y plantear la situación actual de la ubicación del cuarto de equipos y la analizar la reubicación del cuarto de equipos.

- Coordinar la implementación de niveles de acceso físico al cuarto de equipos, mediante la revisión de ingreso de objetos y registro por bitácora del personal que accede al cuarto de equipos con autoridad de la manipulación de los activos.

- Seguir el Hardening propuesto de implementaciones de seguridad física en el cuarto de equipos (Véase anexo 8).

- Implementar los controles de acceso apoyándose en las mejores prácticas de la ISO 27002, de acuerdo al tamaño de proyecto, colocando seguridades físicas como candados y sellos de seguridad en los equipos.

- Implementar controles magnéticos para que solo el personal autorizado pueda acceder al cuarto de equipos.

**Propuesta de contingencia**

La propuesta de contingencia será aplicada en caso de que todavía se presente el riesgo, los pasos son los siguientes:

- Revisar las debilidades encontradas luego de aplicar la medida preventiva.

- Revisar los controles de acceso definidos al cuarto de equipos (gerencia, administrativo, administrador de red).

- Implementar nuevas medidas preventivas en función a las debilidades encontradas.

- Documentar las nuevas medidas preventivas.

- Implementar sanciones al personal en caso de no cumplir con las políticas.

**Involucrados**

- Administradora de la red.
- Proveedor TE UNO.
- Gerencia del proyecto.
- Personal administrativo.

2. Realizar un análisis de implementación de redundancia de energía eléctrica e implementación de mejores prácticas para realizar el levantamiento y organización en el cuarto de equipos con el fin de mejorar la calidad y la gestión de los equipos.

**Probabilidad de riesgo al no aplicar la medida preventiva**

Telefónica ha contratado al proveedor un servicio 24 x 7, es decir sin interrupción, el riesgo que se puede tener es fallas de cortes eléctricos y desconexión de la continuidad en el servicio brindado, pérdida de información no almacenada, Daños en los equipos (Hardware), sanciones con el cliente debido a que la disponibilidad del servicio no es brindada al 100 % como indica el contrato firmado.

**Cumplimiento a la medida preventiva**

- Implementar redundancia en la energía eléctrica.
- Implementar una topología de UPS.
- Difundir las políticas al personal autorizado al cuarto de equipos.

**Recomendaciones luego de aplicar la medida preventiva**

- Mantener una reunión con gerencia y plantear el problema que podría causar al no tener redundancia de energía eléctrica y definir conjuntamente la implementación de la misma.

- Implementar el UPS para redundancia de energía eléctrica, utilizando una topología que asegure la energía por algún tiempo.

- Documentar políticas en función a las mejores prácticas para la organización del cuarto de equipos.

- Realizar una reorganización de los patch cord en función a las especificaciones técnicas para instalación de cableado estructurado.

- Realizar etiquetado de cada uno de los patch cord para identificar rápidamente las conexiones correspondientes.

- Documentar los cambios realizados en el cuarto de equipos con el fin de realizar un Rollback en el caso de que el cambio a realizar no sea exitoso.

**Propuesta de contingencia**

- Analizar el problema tiempos de indisponibilidad y respuesta a la misma.

- Analizar el grado de criticidad del error presentado.

- Evaluar las acciones de respuesta tomadas en el momento.

- Revisar los UPS existentes revisando que se encuentren funcionando correctamente.

- Identificar, definir y analizar las vulnerabilidades encontradas en el cuarto de equipos para mejorar eventualidades por fallas eléctricas.

**Involucrados**

- Administradora de la red.
- Proveedor TE UNO.
- Gerencia del proyecto.
- Personal administrativo.

**Procedimientos**

1. Realizar un proceso de revisión a la documentación existente para el proyecto que permita identificar procedimientos útiles al servicio y permitir la elaboración de nueva documentación, luego de ello se deberá definir un plan de difusión en el personal del Service Desk con el fin de que el equipo conozca, y sobre todo aplique la documentación en la gestión diaria evitando con ello el mal uso de información.

**Probabilidad de riesgo al no aplicar la medida preventiva**

Desorden en los procedimientos y acciones que se realizan dentro de las áreas que conforman el Service Desk, manejo irresponsable de procedimientos y documentación existente para el servicio provocando incumplimiento a las normas impuestas por el cliente.

**Cumplimiento a la medida preventiva**

- Revisar documentación existente de procedimientos en función del servicio para reconocer la alineación entre políticas y procedimientos.

- Elaboración de documentación faltante.

- Solicitar la aprobación de la gerencia y difundir la documentación según la metodología de difusión establecido en el proyecto.

- Definir un proceso de revisión de cumplimiento a lo normado en la documentación.

- Establecer un mecanismo de registro de incumplimiento a las normas, procesos y procedimientos para el análisis y toma de decisiones.

**Recomendaciones luego de aplicar la medida preventiva**

- Realizar un análisis de procedimientos versus políticas para verificar el alineamiento de la documentación.

- Coordinar con el cliente la creación de documentación, en caso de ser necesario, que norme el manejo del servicio.

- Solicitar la aprobación por parte del cliente y gerencia de TCS del proyecto.

- Definir un método de registro de incumplimiento a las normativas documentadas.

- Realizar un análisis trimestral para conocer el grado de cumplimiento del personal mediante evaluaciones On line, encuestas u otros.

- Al implementar las medidas preventivas realizar un documento de control de cambios, es decir versiones de cada actualización de los procedimientos existentes.

- Implementar un documento que permita identificar la ruta o path correspondiente de cada uno de los procedimientos.

**Propuesta de contingencia**

Si el problema se presenta se tendrá como procedimiento de revisión el siguiente:

- Definir gravedad del error y responsabilidades según documentación definida.

- Restablecer funciones durante las revisiones.

- Recolectar toda la documentación posible y revisar si su implementación podría haber mitigado el riesgo ocurrido.

- Definir responsables de la información y documentación así como el procedimiento que tuvo el error.

- Definir la alineación entre la documentación y el conocimiento de la misma entre el personal.

- Definir el incumplimiento que hubo o falla en la documentación existente.

- Definir el plan de acción para corrección del incumpliendo y sanción al personal que lo incumplió.

- Presentar al cliente el análisis y medidas tomadas para su aprobación.

**Involucrados**

- Contraparte de Telefónica.
- Personal del Service Desk.
- Gerencia del proyecto.

**Personal**

1. Realizar una capacitación al personal tanto nuevo como antiguo con la intención de concientizar la seguridad en la información, dar a conocer documentación existente para la entrega del servicio a Telefónica y entregar Tips de mejores prácticas que podrían ser implementadas y mejorar la calidad del servicio.

**Probabilidad de riesgo al no aplicar la medida preventiva**

Manejo irresponsable de información, al no conocer lo delicada que puede ser una información su manipulación por parte del colaborador puede ser irresponsable es decir podría ser alterada sin razón o entregada a personas externas al servicio ocasionando difusión o perdida de la información, lo cual terminaría en un proceso

legal ya que la empresa Telefónica maneja información de clientes y datos sensibles, este riesgo podría presentarse al final como un problema legal.

**Cumplimiento a la medida preventiva**

- Solicitar al área de Recursos Humanos TCS la autorización para la capacitación al personal y ayuda a la organización de la misma.

- Coordinar con el área de Seguridad Informática la ayuda para que en la capacitación se concientice en el personal la seguridad a la información que se maneja.

- De entre el personal que brinda el servicio escoger al más antiguo que conozca donde se encuentra la documentación y forma de brindar el servicio, para seleccionar temas importantes y de ayuda al proyecto.

- Unificar información y armar módulos de capacitación.

- Definir tiempos de revisión y cumplimiento a las buenas prácticas entregadas al operador.

**Recomendaciones luego de aplicar la medida preventiva**

Unificar información y armar módulos de capacitación, el expositor deberá ser alguien que conozca del negocio y se prepare en los temas a tratar que deberían ser:

- Importancia de la seguridad en la información dentro del proyecto.

- Clasificación de la información utilizada y manipulada por el personal de las diferentes áreas del proyecto.

- Concientización de la visión y misión del proyecto Service Desk.

- Presentación de documentación normante para el proyecto proporcionada por Telefónica.

- Presentación de manuales útiles para la entrega del servicio otorgado por Telefónica.

- Presentación de documentación normante para el proyecto proporcionada por TCS.

- Presentación de manuales y procedimientos autorizados útiles para el servicio otorgados por TCS.

- Propuesta de mejores prácticas para la entrega del servicio.

- La revisión del cumplimiento podría ser evaluado cada 6 meses mediante la revisión de bitácoras de incumplimiento y pruebas de conocimiento que permitan medir el grado de conocimiento de los colaboradores.

**Propuesta de contingencia**

La propuesta de contingencia es una propuesta en caso de que pese a las prevenciones y controles colocados se presenta el riesgo, y se difunda información sensible a terceros (personal externo al proyecto).

- Se deberá definir el alcance del riesgo según la información que se filtró o que tuvo alteración.

- Se deberá solicitar al cliente los log de aplicaciones y servidores que manejan o alojan dicha información, ya que los mismos alojan datos del usuario que realiza las consultas a la base, con fechas y hora de consultas o modificaciones.

- Se revisará toda la documentación existente para identificar si en alguna existe el impedimento de la acción realizada y si existe alguna excepción al impedimento.

- Validar entre el personal el desconocimiento a lo normado por el cliente y TCS.

- Definir responsabilidades según la evidencia levantada.

- Determinar sanciones y entrega de evidencias al caso legal que se presente.

**Involucrados**

- Personal del Service Desk.
- Gerencia del proyecto.
- Cliente Telefónica.

**Condiciones de implementación**

Para la implementación de las medidas preventivas descritas en el plan de prevención debe cumplirse con ciertas condiciones que harán factible la implementación:

- El compromiso de las áreas involucradas.

- El compromiso y autorización del cliente para la revisión de aplicaciones, logs y documentación existente.

- Disponibilidad del personal para las entrevistas y capacitaciones.

- Predisposición del personal para poner en práctica y mantener la difusión de lo aprendido.

- Predisposición de la gerencia del proyecto para gestionar a lo interno las acciones necesarias para regularizar y aplicar las medidas preventivas.

- Coordinación con el proveedor TE UNO para las capacitaciones solicitadas.

- Disponibilidad de seguridad informática, administrador de red para la implementación de nuevas medidas.

**Conclusiones**

- El aplicar las medidas preventivas permitirá al servicio mejorar la seguridad en la información que se maneja dentro del proyecto.

- Definir un plan de prevención permitirá al proyecto actuar de manera oportuna ante riesgos y vulnerabilidades de lo encontrado en el análisis inicial.

- No se tiene un 100 % de seguridad de reducir el riesgo al aplicar las medidas preventivas debido a que la seguridad abarca muchos ámbitos más y ningún sistema, aplicación, red, es segura, sin embargo se tiene una propuesta de contingencia con el objetivo de reducir el riesgo en el caso de que se pueda detectar nuevas vulnerabilidades.

- Teniendo un plan de contingencia también se puede tener planes de acción en caso de inconvenientes críticos para el servicio.

**Justificación**

La informática forense es una metodología relativamente nueva, fundamentada o conocida como: *"Una ciencia que busca reproducir científicamente con una metodología estricta de los hechos acontecidos y su correlación para determinar el grado de impacto, y posteriormente establecer en coordinación con otros entes intervinientes, mecanismos tendientes a evitar nuevamente su ocurrencia, que van desde el marco normativo hasta la utilización de mecanismos técnicos".* (Luis ángel Gómez, 2012)

En función de esto la informática forense es una metodología aplicada para cuando ocurre un evento y este debe ser analizado en su causa y origen, por teoría y revisión la informática forense indica que es aplicable al hardware y software del evento ocurrido, durante el desarrollo de las medidas de prevención para el proyecto Service Desk de Telefónica se ha determinado 4 ámbitos de revisión los mismos que son Red Interna, procedimientos, personal e instalaciones, por lo descrito podemos ver que solo red interna podría aplicar informática forense en sus revisiones.

La informática forense no tiene un lineamiento a cumplir ni un esquema de aplicación, es mundialmente usada para obtener causa y efecto de un evento, pero también puede ser aplicable para medidas preventivas, la informática forense indica una revisión inicial, un análisis de información y una entrega de resultados. Teniendo como antecedente esta definición, se ha realizado un estudio al proyecto Service Desk de Telefónica aplicando informática forense para el diseño de medidas preventivas.

Lo primero que se realizó es una revisión inicial para lo cual se aplicó marcos de referencia de auditoria en seguridad informática como son COBIT, ISO27002 e ITIL, luego de esto se realiza un análisis de la evidencia obtenida y se emiten las medias preventivas. Las medidas de prevención descritas están basadas en informática forense, la misma que por teoría indica solo hardware y software.

Los ambientes revisados que no contienen hardware y software son procedimientos, personal e instalaciones, sobre ellos también se aplica el mismo procedimiento de revisión, emisión de medias preventivas, y planes de contingencia, esto tomando en cuenta que son la base y normativa para el buen funcionamiento del hardware y software existente en el proyecto Service Desk. El buen funcionamiento de la red interna y en si del proyecto va ligado directamente a estos ámbitos puesto que determinan como, donde y quien es el responsable de la información que se maneja en el proyecto. Si se aplica de forma efectiva las medidas preventivas en estos ámbitos el hardware y software estará funcional de forma segura.

Es así como se determinó anteriormente, la informática forense no tiene una metodología específica para realizar el diseño de medidas preventivas, es por eso que se ha podido apoyar directamente en los marcos de referencia de seguridad informática. Según Alexandra Jácome la informática forense busca prevenir el cometimiento de los delitos apoyándose en la seguridad informática. (Elizabeth, Jácome Ortega Alexandra, 2011)

### 3.5. Presentación del proyecto

Las medidas preventivas expuestas anteriormente tienen el objetivo de reducir el riesgo actual del Service Desk tomando en cuenta que las vulnerabilidades detectadas

pueden convertirse en un problema informático que pueda incurrir costos al proyecto.

Partiendo de este punto, la medida preventiva crítica que debe ser ejecutada inmediatamente es el Hardening expuesto por TCS para obtener la certificación de seguridad informática, para ello se ha diseñado un Hardening macro en función a las observaciones de la situación actual del proyecto, se recomienda su ejecución en el Service Desk 3 veces por año, tomando en cuenta que la versión puede cambiar según las vulnerabilidades detectadas y la actualización del documento.

Previo a la ejecución del Hardening se deberá obtener la aprobación del personal involucrado: gerencia, administrador de red, jefatura de soporte en sitio, seguridad informática. (Véase anexo # 8)

### 3.5.1. Indicadores para medir la viabilidad del proyecto

A continuación se procede a detallar indicadores para medir la viabilidad del presente proyecto, cabe indicar que se deberá dar seguimiento sobre la factibilidad técnica de implementación de medidas preventivas apoyadas en la informática forense a través de las herramientas de software libre y así recomendar a diferentes áreas la implementación del mismo para prevenir incidentes de seguridad informática.

- Medir la situación actual de la empresa referente a seguridad informática y luego de 3 meses conocer si se redujo los riesgos mediante la operación del presente proyecto.

- Verificar el número de vulnerabilidades detectadas por mes.

- Verificar el número de vulnerabilidades resueltas por mes.

- Realizar un análisis causal sobre las vulnerabilidades más críticas y tomar planes de acción sobre el mismo.

- Llevar un control estadístico comparativo de los resultados obtenidos en relación a empresas que brinden servicios similares.

- Adicional mediante la viabilidad del proyecto se podrá recomendar a diferentes áreas la implementación de la propuesta.

## CONCLUSIONES

- Después de realizar el análisis de la situación del Service Desk se pudo evidenciar vulnerabilidades en los ámbitos de: red, instalaciones, procedimientos, personal. Como consecuencia, es evidente un riesgo probable a la información interna y del cliente.

- Al estudiar las herramientas de informática forense, se puede concluir que sirven para 2 ámbitos específicos: diagnóstico en función a un problema ocurrido, detección y prevención de vulnerabilidades.

- El servicio no cuenta con un plan de mantenimientos de los equipos, el 90 % del personal trabaja en la operatividad diaria estando expuesta a riesgos de seguridad informática.

- El diseño de medidas preventivas ayudará a mitigar el riesgo y reducir el impacto de un problema informático, sin embargo no se garantiza que no se tenga problemas de seguridad en la producción del proyecto.

- El ejecutar las medidas preventivas ayudará al proyecto a mejorar la gestión de la seguridad de información de una manera adecuada en función a los marcos de referencia ISO 27002, COBIT 4.1, ITIL V3 para garantizar los puntos importantes integridad, confidencialidad, disponibilidad.

- Con el estudio realizado se puede concluir que la seguridad no es solo implementar sistemas de seguridad, si no abarca muchos ámbitos más, es decir para asegurar la integridad, disponibilidad, confidencialidad se debe analizar la red interna, las instalaciones, los procedimientos, el personal tal cuál fue definido en la presente tesis con la finalidad de emitir planes de acción para reducir el riesgo.

## RECOMENDACIONES

- La gerencia a nivel de TCS debe difundir y concientizar al personal sobre la importancia de la seguridad en el uso eficiente y responsable de la información.

- Adaptar a la organización a las mejoras prácticas de ITIL con la finalidad de identificar posibles problemas que permita mejorar las políticas y procedimientos de la empresa.

- Se recomienda verificar los niveles de acceso de los usuarios para garantizar los puntos principales de la seguridad de la información: integridad, confidencialidad, disponibilidad.

- Se deberá realizar un análisis de vulnerabilidades cada 3 meses especialmente en los equipos críticos, aun cuando no exista inconvenientes detectados al aplicar el Hardening propuesto en la presente tesis.

- Documentar nuevas medidas preventivas en el Hardening en el caso de que sean detectadas al realizar un análisis de vulnerabilidades.

- Se debe suscribir a páginas de seguridad especializada para conocer las últimas vulnerabilidades reportadas y tomar las medidas necesarias si es el caso.

- Se recomienda elaborar un documento aprobado por un comité superior en el cual conste las responsabilidades y políticas que tiene que cumplir el personal con respecto a la seguridad de información.

- Como recomendación de seguridad es importante empezar a llevar registros sobre incidentes de seguridad con el fin de dar mayor confiabilidad y mejorar los resultados en el ciclo de vida del análisis de riesgos.

## LISTA DE REFERENCIAS


Alegsa. (11 de mayo de 2010). *Alegsa.com.ar*. Recuperado el 13 de enero de 2015, de Alegsa.com.ar: http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Arturo Palacios Ugalde. (octubre de 2010). Recuperado el 3 de marzo de 2015, de http://www.sepi.esimez.ipn.mx/msistemas/archivos/Palacios%20Ugalde%20Arturo.pdf

Belloso Ramiro. (noviembre de 2008). *Repositorio Institucional*. Recuperado el 28 de enero de 2015, de Universidad del Savlador sistema bibliotecario: http://ri.ues.edu.sv/3190/1/Estudio%20y%20an%C3%A1lisis%20sobre%20la%20inform%C3%A1tica%20forense%20en%20El%20Salvador.pdf

Bormart. (2009-2012). *Red Seguridad*. Recuperado el 28 de diciembre de 2013, de http://www.redseguridad.com/opinion/articulos/sabes-diferenciar-la-iso-27001-y-la-iso-27002

Data Recover Center. (2014). Recuperado el 2 de julio de 2013, de http://www.datarecovercenter.co/Servicios/Informatica-Forense/Auditoria-e-Investigacion-Forense/Historia-de-la-Informatica-Forense

Eduardo Federico Santillan. (2010). *Paraiso Linux*. Recuperado el 10 de abril de 2015, de Paraiso Linux: http://paraisolinux.com/que-es-y-como-usar-nmap/

Elizabeth, Jácome Ortega Alexandra. (julio de 2011). *dspace.pucesi.edu.ec.* Obtenido de dspace.pucesi.edu.ec: http://dspace.pucesi.edu.ec/bitstream/11010/172/1/T72592.pdf

Elizabeth, Jácome Ortega Alexandra. (2011). *Pontificia Universidad Católica del Ecuador.* Recuperado el 27 de 01 de 2014, de http://dspace.pucesi.edu.ec/bitstream/11010/172/1/T72592.pdf

Enrique Martínez – Salanova Sánchez. (2012). *Portal de la educomunicación*. Recuperado el 03 de enero de 2015, de uhu.es: http://www.uhu.es/cine.educacion/index.htm

Expansión. (2014). Recuperado el 11 de marzo de 2014, de http://www.expansion.com/diccionario-economico/tasa-interna-de-retorno-o-rentabilidad-tir.html

Fidias Arias. (2004). *oocities.org*. Recuperado el 03 de febrero de 2015, de oocities.org: http://www.oocities.org/es/annadugarte/seminario/Metodologia.htm

forense, Informática. (2010). *Informática forense*. Recuperado el 21 de junio de 2013, de http://www.informaticaforense.com.ar/informatica_forense.htm

Gambeta. (25 de octubre de 2011). *Gambeta*. Recuperado el 10 de abril de 2015, de Gambeta: http://www.genbeta.com/a-fondo/conan-la-herramienta-gratuita-de-analisis-de-inteco-ha-sido-actualizada-a-fondo

Giovanni Zuccardi y Juan Gutierrez. (2006). Recuperado el 27 de 01 de 2014, de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Icontec. (16 de noviembre de 2007). *Icontec Internacional*. Recuperado el 13 de enero de 2015, de Tienda icontec.org: http://tienda.icontec.org/brief/NTC-ISO-IEC27002.pdf

Informática forense. (11 de octubre de 2006). Recuperado el 12 de julio de 2013, de http://www.informaticaforense.com.co/index.php?option=com_content&view=article&id=22&Itemid=34

Informática forense. (10 de septiembre de 2013). Obtenido de http://forencenbcruzh.wordpress.com/2013/09/10/rfc-3227/

Informática frustrada. (2005). *Informática frustrada*. Recuperado el 13 de enero de 2015, de Informáticafrustrada.es: http://informaticafrustrada.es/tag/error-informatico/

Inteco. (2011). Recuperado el 27 de febrero de 2014, de https://conan.cert.inteco.es/analizador.php

Inteco. (25 de octubre de 2011). *Gambeta.com*. Recuperado el 13 de enero de 2015, de Gambeta: http://www.genbeta.com/a-fondo/conan-la-herramienta-gratuita-de-analisis-de-inteco-ha-sido-actualizada-a-fondo

ISO/IEC. (16 de noviembre de 2007). *ISO27000.* Recuperado el 5 de enero de 2015, de NORMA TÉCNICA NTC-ISO/IEC: http://tienda.icontec.org/brief/NTC-ISO-IEC27002.pdf

IT Governance Institute. (2007). *IT Governance Institute.* Recuperado el 13 de enero de 2015, de itgi.org: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

IT GOVERNANCE INSTITUTE. (2008). *ISACA.* Obtenido de ISACA.ORG: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

ITIL V3. (2011). Recuperado el 26 de febrero de 2014, de http://itilv3.osiatis.es/gestion_servicios_ti.php

Javier ituurioz. (2014). Recuperado el 04 de marzo de 2014, de http://www.expansion.com/diccionario-economico/valor-actualizado-neto-van.html

José Luis Rivas López. (03 de febrero de 2015). *Ordenadores y portátiles.* Obtenido de Informática forense: http://webs.uvigo.es/jlrivas/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

José Manuel Ferro Veiga. (s.f.). *Investigación criminal* . Recuperado el 19 de febrero de 2015, de https://books.google.com.ec/books?id=MHqUBgAAQBAJ&pg=PT70&dq=Es+importante+conocer+los+antecedentes,+situaci%C3%B3n+actual+y+el+proceso+que+se+quiere+seguir+para+poder+tomar+la+mejor+decisi%C3%B3n+con+respecto+a+las+b%C3%BAsquedas+y+la+estrategia+de+inves

Laura Isabel Sainz Miranda. (8 de diciembre de 2007). *Auditoría sistemasucb.* Recuperado el 17 de marzo de 2015, de Auditoría sistemasucb: http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10

&cad=rja&uact=8&ved=0CE4QFjAJ&url=http%3A%2F%2Fauditoriasistemasucb.pbworks.com%2Ff%2FInform%25C3%25A1tica%2BForense.docx&ei=uscIVdKqFYqnyASatYFw&usg=AFQjCNEO-XPGMSUW01QyNANUyW6bNX-dRA&bvm=

Lenox. (s.f.). *Sistemas Lenox.* Recuperado el 11 de abril de 2015, de Sistemas Lenox: http://www.sistemaslenox.com.ar/helplenox/Pyme/recomendaciones_para_cableado_.htm

Lizeth Arely. (30 de enero de 2014). *Arely*. Recuperado el 09 de marzo de 2015, de Arely: http://lizeht-arely.blogspot.com/2014/01/informatica-forense-es-el-evidencias.html

Luis ángel Gómez. (2012). *minseg.* Recuperado el 23 de enero de 2015, de minseg.gob.ar: http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.minseg.gob.ar%2Fdownload%2Ffile%2Ffid%2F893&ei=RZrrVIa3OYfjsATN74AI&usg=AFQjCNEY_VwC5WHrMlZw28NJmeexMeY5Xg&sig2=_K6mbs1CSeieFz4E7_43_g&bvm=bv.86475890,d.e

MacAfee. (2013). Recuperado el 25 de febrero de 2014, de http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf

Mendoza Andrea. (25 de octubre de 2014). *Mendoza*. Obtenido de https://prezi.com/shclehxykbqc/principales-problemas/: https://prezi.com/shclehxykbqc/principales-problemas/

Métodos y Técnicas de auditoria informática. (8 de junio de 2013). Recuperado el 1 de abril de 2014, de http://www.slideshare.net/ShamyNavarrete/mtodos-y-tcnicas-de-auditoria-informtica

Microsoft. (2015). *Microsoft.* Recuperado el 11 de abril de 2015, de Microsoft: http://www.microsoft.com/en-us/download/details.aspx?id=7558

Milenium. (2008). Recuperado el 25 de febrero de 2014, de http://www.soporteremoto.com.mx/help_desk/articulo04.html

Mota, J. M. (2013). *Criminalistíca*. (C. M. Mota, Editor) Recuperado el 1 de diciembre de 2014, de Criminalistíca Web Site: http://criminalistica.mx/areas-forenses/audio-video-y-fotografia/1101-ique-es-la-informatica-forense-o-forensic#page

NimboSystem. (3 de mayo de 2013). *NimboSystem*. Recuperado el 13 de enero de 2015, de NimboSystem: http://nimbosystems.com/wp/?p=52

Nmap. (2013). *http://nmap.org/*. Recuperado el 13 de enero de 2015, de http://nmap.org/

Osvaldo Puello Flores. (2008). *Universidad del Norte*. Recuperado el 28 de 02 de 2014, de http://manglar.uninorte.edu.co/bitstream/handle/10584/2209/Operaci%C3%B3n%20del%20servicio.pdf?sequence=1

Perícia Forense aplicada a informática. (1 de octubre de 2003). Recuperado el 1 de abril de 2014, de https://br.groups.yahoo.com/neo/groups/PericiaForense/conversations/messages/1020

Ramírez, G. (2008). *La Consigna*. Recuperado el diciembre de 2014, de http://laconsigna.wordpress.com/2008/05/26/informatica-forense/

Revista Red. (Noviembre de 2002). *Seguridad informática*. (R. Red, Editor) Recuperado el 5 de enero de 2015, de Informática y programación: http://martomontes.jimdo.com/seguridad-informatica/

Roger Carhuatocto. (2008). Recuperado el 25 de 02 de 2014, de http://cp4df.sourceforge.net/

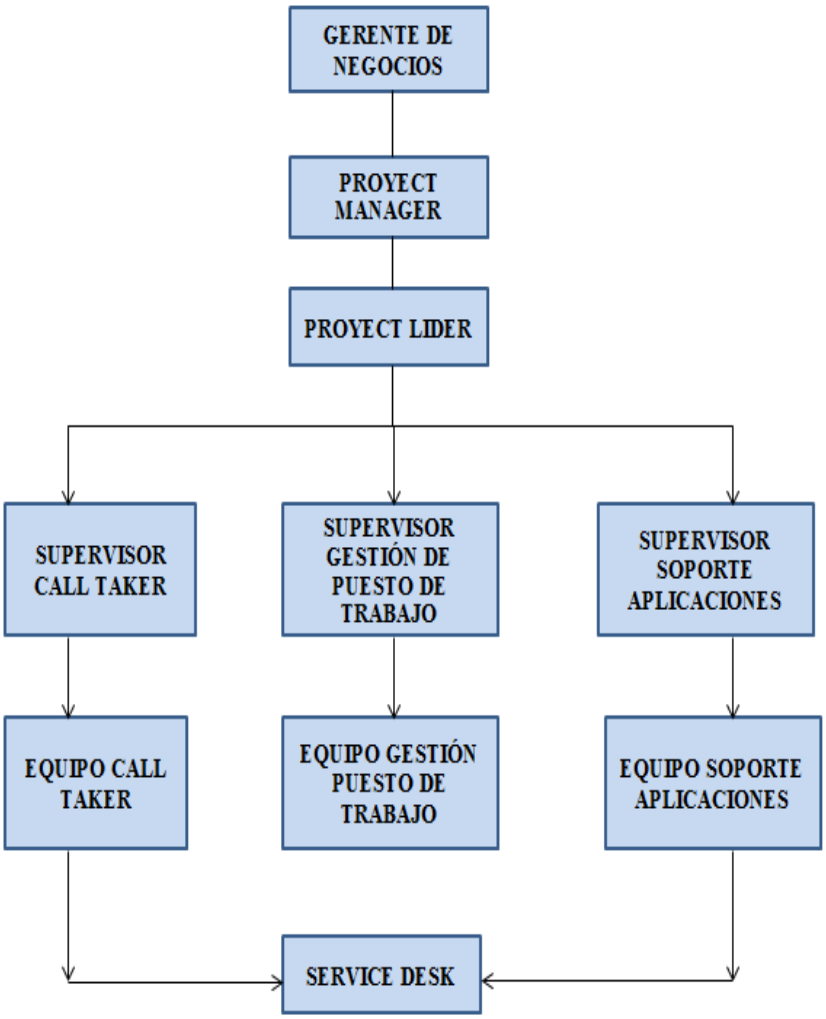
Telefónica. (2013). *Telefónica*. Recuperado el 31 de 05 de 2013, de http://www.telefonica.com.ec

Transforma Consultoría. (2012). *Transforma Consultoría*. Recuperado el 17 de marzo de 2015, de Transforma Consultoría: http://www.transformaconsultoria.com/index.php/component/content/category/9-noticias

UTN-FICA-EISIC. (s.f.). Recuperado el 25 de 02 de 2014, de http://repositorio.utn.edu.ec/bitstream/123456789/539/21/04%20ISC%20157%20RESUMEN%20TECNICO%20ESPA%C3%91OL.pdf

# ANEXOS

Anexo 1. Estructura organizacional



Anexo 2. Entrevista para el levantamiento de información de la situación actual del Service Desk

**Entrevista para la descripción actual del Service Desk**

**Persona entrevistada:** Líder del proyecto

**Responsable:** Henry Chacón

**Fecha:** 12 de Noviembre 2014

**Preguntas**

1. ¿Qué servicios brinda la empresa TATA?
2. ¿En dónde se encuentra ubicado el servicio de Service Desk prestado por la empresa TATA?
3. ¿Cuáles son los servicios acordados con el cliente para el servicio de Service Desk? ¿Cuál es la función de cada servicio?
4. ¿Mantiene una estructura organizacional del servicio Qué servicios presta a la empresa Telefónica como mesa de ayuda?
5. ¿Cuál el hardware y software que cuenta el servicio de Service Desk?
6. ¿Cuál es el hardware de red que cuenta el servicio?
7. ¿Cuenta con telefonía en el servicio de Service Desk?
8. ¿Cales son las aplicaciones comúnmente que se utiliza en el servicio?
9. ¿Con cuantas personas cuentan para brindar el servicio?

Anexo 3. Encuesta al personal sobre seguridad de la información ENC001


**Objetivo de la entrevista:**

Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de robo, fraude o uso inadecuado de la información.

**Preguntas**

**Comunicación**

1. ¿Conoce políticas internas para la clasificación de la información?

2. ¿Conoce de políticas para la clasificación de los tipos de acceso a la información (lectura, escritura)?

**Documentación**

1. ¿Conoce la clasificación de información existente en el cliente y su empresa propia?

2. ¿Conoce manuales de procesos técnicos que estén alineados a los objetivos empresariales?

3. Cuenta con manuales de procesos de administración de aplicaciones que estén alineados a los objetivos empresariales

**Gestión de incidentes**

4. ¿Tiene establecido escalas de tiempo para el manejo de incidentes?

5. ¿Cuenta con un procedimiento basado en escalamientos para el manejo de un incidente?

6. ¿Se realiza un análisis inicial del incidente por parte del Service Desk?

7. ¿Para el análisis inicial del incidente cuenta con una herramienta o una base de conocimiento?

8. ¿Una vez dada una solución al incidente se confirma el funcionamiento con la realización de pruebas en el nivel de escalamiento que se encuentre?

**Gestión de problemas**

9. ¿Realiza investigación de las causas que generaron los incidentes?

10. ¿Realiza la identificación de la causa raíz de los problemas y propone soluciones definitivas?

11. ¿Realiza la identificación de la causa raíz de los problemas y propone soluciones temporales?

12. ¿Mantiene actualizado el registro de problemas y errores (errores conocidos) con soluciones temporales hasta su solución definitiva?

13. Control de Problemas y Errores

14. ¿Usted instala software en su computador que no use para su jornada laboral?

15. ¿Comparte su contraseña de inicio de sesión del computador con los compañeros de trabajo?

16. ¿Conserva registros de las contraseñas en (papel, archivos de software,)?

17. ¿Usa dispositivos de almacenamiento externo para extraer información del computador que usa en la empresa?

18. ¿Conoce si en la empresa tienen un proceso de Backups de información relevante continuo?

19. ¿Cuenta con reglamento de seguridad informática para el usuario?

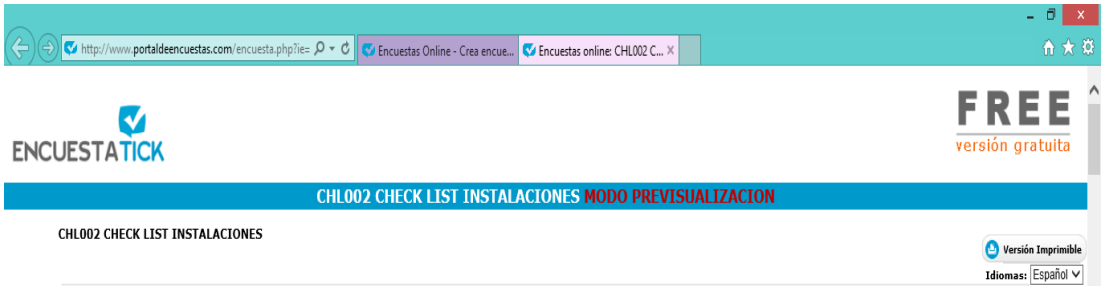
20. ¿Cuenta con copias de los documentos almacenados en el fileserver?

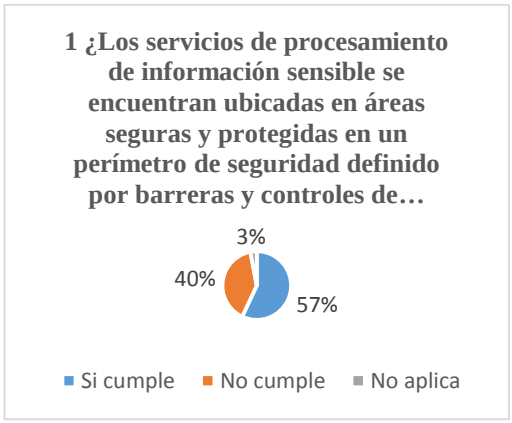
21. ¿Se tienen establecidos procedimientos de actualización a estas copias?

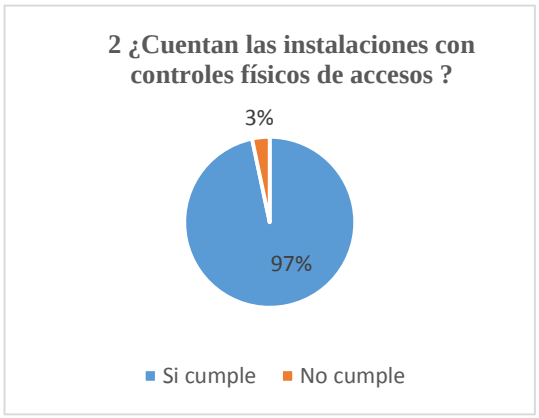
22. ¿Se tiene controles para instalar software no autorizados por la empresa?

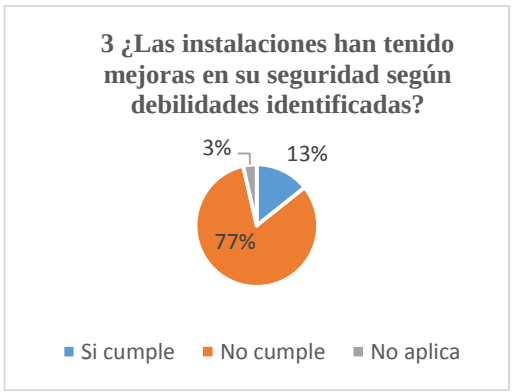
23. ¿Cuentan con algún tipo de control de entradas y salidas de usuario?

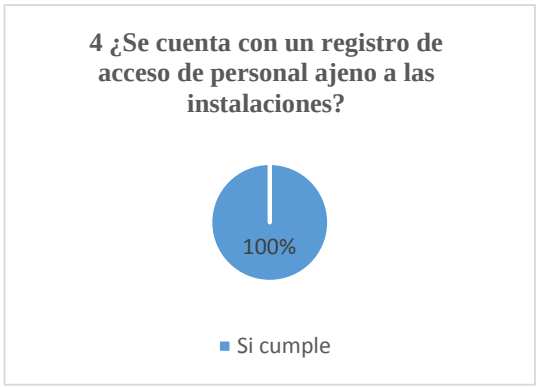
Anexo 4. Check List de Instalaciones CHL002

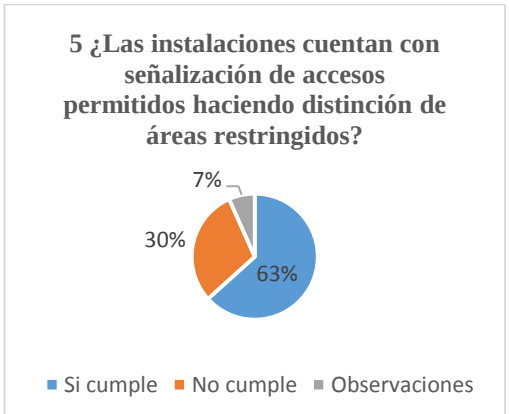


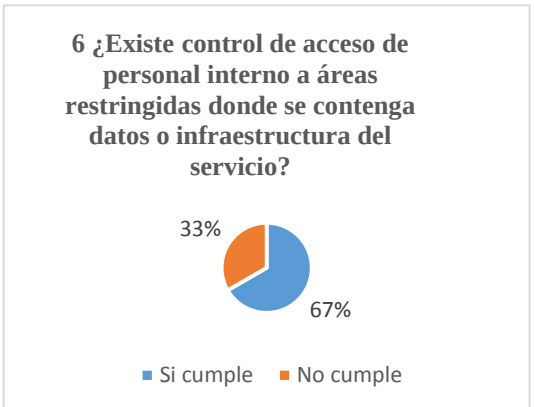



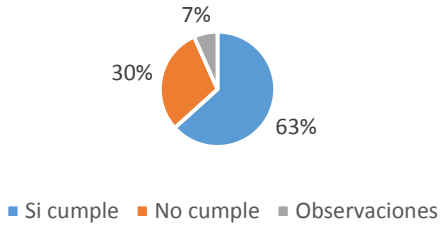



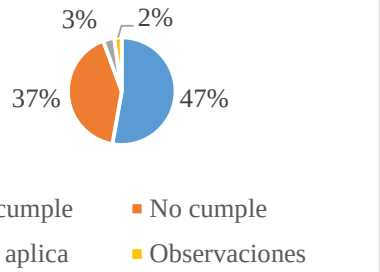



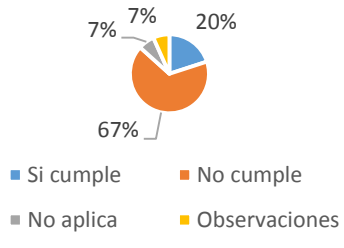
**7 ¿Se ha restringido el área donde se encuentra en funcionamiento la infraestructura de red del Service Desk?**



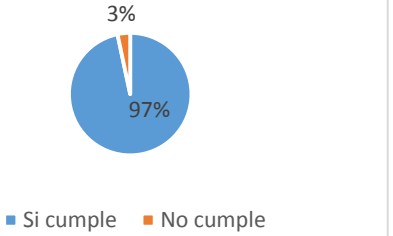

8 SEGURIDAD DE LOS EQUIPOS
¿El cuarto de equipos cuenta con protección física a los equipos?



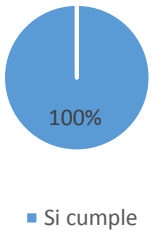

**9 ¿Se cuenta con controles de temperatura dentro del cuarto de equipos?**



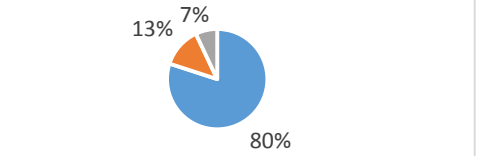

**10 ¿En las instalaciones se cuenta con señalización en caso de emergencia?**



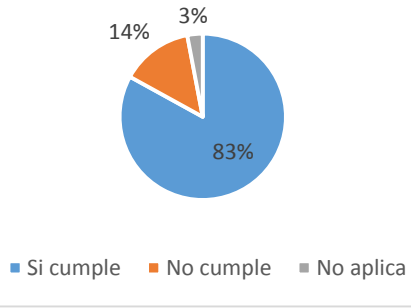

**11 ¿Se cuenta con extintores o sistema contraincendios en base de gas?**



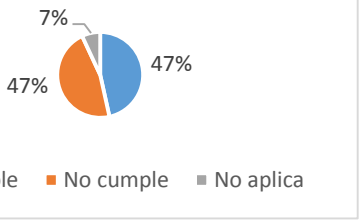

**12 ¿Antes del ingreso al cuarto de equipos el personal de seguridad realiza el chequeo necesario para evitar el ingreso de material innecesario?**



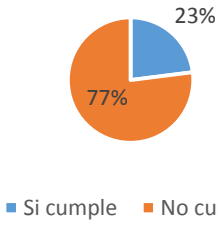

**13 ¿Usan códigos de barra para hacer los chequeos mas eficientes sobre los equipos?**



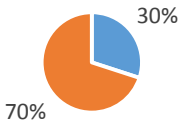

**14 ¿Se sitúa el equipo para protegerse y reducir el riesgo de materialización de las amenazas del entorno así como las oportunidades de acceso no autorizado?**



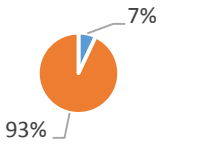
**15 ¿Se protegen los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo?**



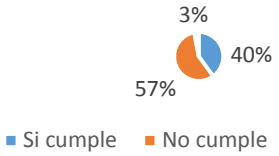

**16 ¿Se protege el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños?**



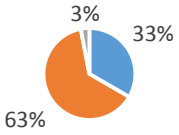

**17 ¿Se realiza el mantenimiento adecuadamente los equipos para garantizar su continua disponibilidad e integridad?**



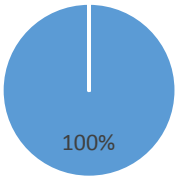

**18 ¿Se aplican seguridades a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos?**



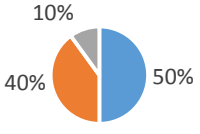

**19 ¿Se revisa cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado…**




**20 ¿Se cuenta con un control de ingreso y salida de equipos de las instalaciones**

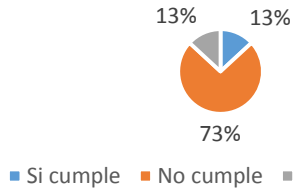



**21 ¿TCS cuenta con procedimientos para el manejo y traslado de equipos que contienen información interna ?**

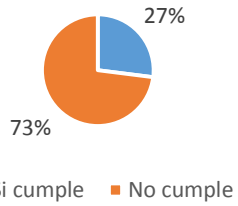



**22 ¿Se cuenta con un circuito cerrado de cámaras de seguridad?**

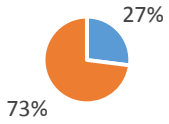
**23 ¿El área donde se encuentran los equipos cuenta con el espacio suficiente para que el personal autorizado pueda desenvolverse en sus trabajos?**



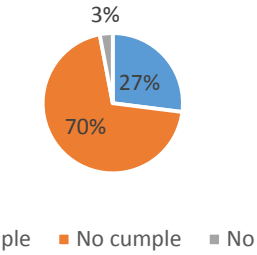

**24 ¿La empresa dispone de controles que permitan proteger la información de amenazas externas y del entorno?**



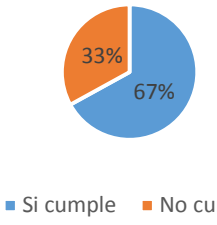

**25 ¿La empresa dispone de controles de seguridad que minimicen daños en el cableado, equipos del centro de datos y cuarto de comunicaciones?**



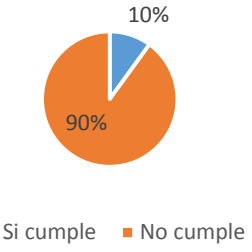

**26 ¿TCS dispone de políticas para la Seguridad en la reutilización o eliminación de equipos ?**



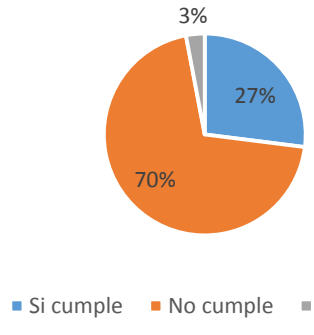

**27 ¿TCS ha definido redundancia en suministro eléctrico?**



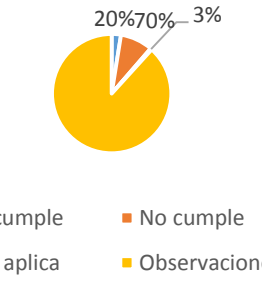

**28 ¿TCS ha definido un plan de mantenimiento de equipos ?**




**29 ¿TCS dispone de un seguro ante incidentes en los equipos críticos?**

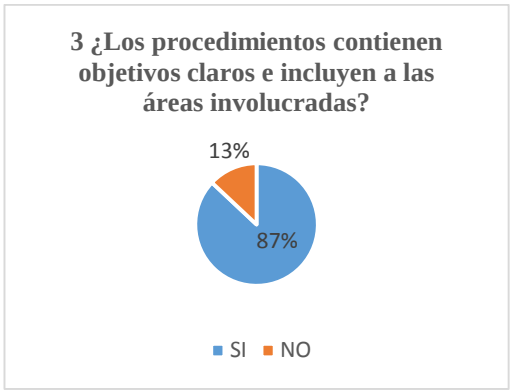


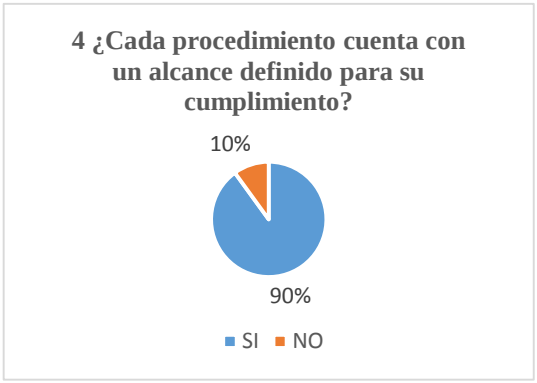

**30 ¿Los cables de datos están dentro de paneles, canales eléctricos y etiquetado correspondiente?**

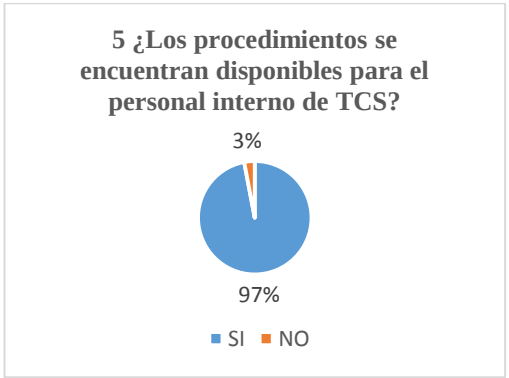


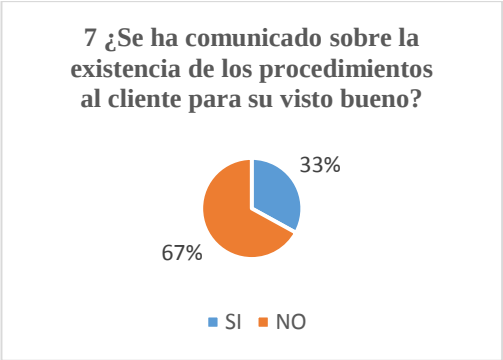
Anexo 5. Check List procedimientos CHL003

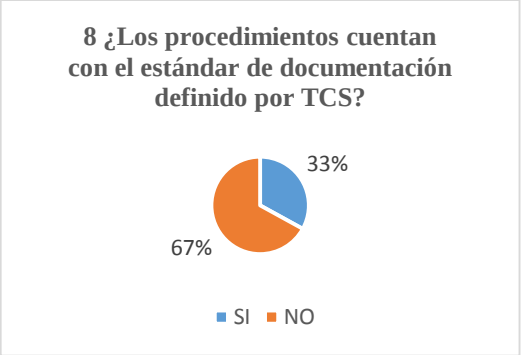




7 ¿Se ha comunicado sobre la existencia de los procedimientos al cliente para su visto bueno?
33%
67%
SI
NO


8 ¿Los procedimientos cuentan con el estándar de documentación definido por TCS?
33%
67%
SI
NO

Anexo 6. Observación directa a personal TOB001

**Revisión a personal**

**RESPONSABLE:** Henry Chacón

Para la revisión se realiza una visita a las instalaciones y se da seguimiento al trabajo continuo de los ingenieros de soporte

TCS como empresa cuenta con procedimientos internos de seguridad los mismos que en su totalidad no ha sido dado a conocer a los colaboradores, en especial al personal del Service Desk por la forma en la que se tomó el servicio.

Los ingenieros de seguridad cuentan con condiciones de trabajo óptimas, necesarias y cómodas para dar el servicio, cuentan con estaciones individuales lo cual les permite resguardar su información personal.

El Service Desk cuenta internamente con 3 áreas dentro de cada una se han definido ciertos procedimientos para el cumplimiento del servicio, pero estos no están aprobados por la gerencia solo son de uso interno de cada área están vigentes pero no están formalizados.

Así también cada área cuenta con una persona que conoce del servicio y tiene la experiencia, esto ayuda a que el personal con menos experiencia pueda aprender las buenas prácticas de la entrega del servicio, planes de capacitación formalizados no se tienen pero por área se ha desarrollado Check List o seguimiento para la capacitación en los temas más relevantes del servicio al nuevo personal.

Los colaboradores más antiguos conocen la ubicación y existencia de los procedimientos tanto de la empresa como del cliente pero por la rotación continua del personal se ha ido perdiendo esta información, y se hace solo de conocimiento verbal no se está retomando a los archivos fuentes, la mayoría de procedimientos que se cumplen son porque así lo han aprendido de los ingenieros de soporte que capacitan. La difusión de nueva información les es enviada vía correo eléctrico con la ruta pero no todo el personal lo revisa.

La comunicación que se tiene con las jefaturas es abierta en el caso de la jefatura inmediata se cuenta con un proceso de escalamiento para emitir sugerencias al servicio en ella está definida que cualquier duda o sugerencia debe realizarse en primera instancia con la persona a cargo del área, y después se seguirá con el escalamiento hasta el Project Leader y en casos extremos se llegaría a la gerencia.

El personal ha sido colocado en cada área por su aptitud y actitud en el desempeño laboral ya que son tres áreas que no requieren el mismo perfil. Se cuenta con la distribución de tareas según el área y lo que norma el contrato para cada área, el supervisor a cargo de cada área es la persona encargada de constantemente difundir en el personal el cumplimiento de procesos y procedimientos internos y del cliente mediante reuniones que se realizan por área mes a mes para a más de estos temas tratar temas del servicio.

Anexo 7. Hardening propuesto de red

**Implementaciones de seguridad de información en el Service Desk**

**Objetivo**

Definir lineamiento de seguridad a cumplir durante la ejecución de medidas preventivas para la corrección de vulnerabilidades.

**Alcance**

Es procedimiento aplica a los sistemas operativos y estaciones de trabajo de la red de la plataforma Microsoft Windows del proyecto de Service Desk.

**Responsables – Participantes**

Soporte en sitio

Seguridad informática

Administración de red

Gestión de usuarios

**Procedimiento general**

**1. Instalación de Microsoft Baseline Security Analyzer**

1.1.Definiciones previas

1.1.1. Descargar el producto de la página oficial de Microsoft para el equipo que se instalara el software.

1.1.2. Realizar la instalación del MBSA (Microsoft Baseline Security Analyzer).

1.1.3. Obtener las últimas versiones autorizadas del MBSA mediante la página oficial.

1.2.Ejecución de software

Realizar el levantamiento del MBSA (Ejecución del software) En la opción de escanear computadoras.

1.2.1. Realizar un análisis de las direcciones IP´s con posibles vulnerabilidades

1.2.2. Ingresar la dirección IP o el rango de direcciones del Service Desk para el análisis correspondiente.

1.3.Informe de Vulnerabilidades

1.3.1. Realizar un análisis del informe emitido por MBSA.

1.3.2. Implementar las recomendaciones emitidas por MBSA.

1.3.3. Documentar las vulnerabilidades encontradas.

**Responsables:** Seguridad informática, administrador de red

**2. Ejecución de actualizaciones**

2.1.Realizar el análisis y documentación de vulnerabilidades de seguridad presentada en los sistemas informáticos Windows, así como los parches que resuelven estas vulnerabilidades.

2.2.Seguridad informática deberá solicitar la aprobación para la ejecución de los parches.

2.3.Una vez obtenida la aprobación realizar la ejecución en un ambiente de pruebas para su evaluación y análisis de impacto.

2.4.Realizar un análisis de los puertos abiertos encontrados y definir los puertos que deberían ser cerrados mediante una plataforma distribuida a cada una de las estaciones de trabajo del Service Desk.

2.5.Realizar la ejecución de actualizaciones mediante una plataforma distribuida a cada una de las estaciones de trabajo del Service Desk.

2.6.Realizar las respectivas pruebas en los sistemas afectados y notificar a los involucrados en el caso de que se presente novedades.

2.7.Soporte en sitio deberá monitorear novedades en las estaciones de trabajo.

2.8.Realizar el informe respectivo de la actualización.

**Responsables:** seguridad informática, soporte en sitio

**3. Configuraciones generales**

3.1.Todo equipo deberá ser configurado en un dominio del directorio activo.

3.2.Configurar el nombre de la computadora en base a los estándares.

3.3.Habilitar políticas de auditoría: administración de cuentas, perfiles, accesos

3.4.Desinstalar componentes de Windows innecesarios en las estaciones de trabajo dependiendo el departamento al que pertenecen y funciones que realizan.

**Responsable:** gestión de usuarios

**4. Recursos compartidos**

4.1. No compartir recursos del sistema innecesarios.
4.2.Remover o eliminar recursos compartidos innecesarios.
4.3.Asignar permisos restrictivos para compartir información.

**Responsable:** seguridad informática, soporte en sitio

**5. Cuentas y grupos de usuarios**

5.1.Verificar que no existan cuentas innecesarias en las estaciones de trabajo.
5.2.Formatear el equipo si va ser utilizado por personal nuevo.
5.3.Las cuentas de usuario que se debe emplear serán usuarios con perfil mínimo, es decir no tendrán perfil de administradores del sistema, a excepción que se demuestre que sea necesario.
5.4.Configurar en Active Directory que la cuenta del usuario sea robusta, mínimo 8 caracteres mediante mayúsculas, minúsculas y números.

**Responsable:** gestión de usuarios, soporte en sitio

**6. Software adicional**

6.1.Instalar y configurar el software antivirus determinado por la empresa con sus definiciones actualizadas.
6.2.Está prohibido instalar software innecesario sin previa autorización del jefe inmediato y el área de Seguridad Informática.
6.3.Todo personal que maneje información confidencial de la empresa o el cliente deberá tener instalado en su estación de trabajo un software de seguridad, se recomienda (SafeBoot).
6.4.Las estaciones de trabajo que mantengan software de seguridad y el equipo sea manipulado por algún técnico, deberá ser notificado a seguridad informática.

**Responsable:** seguridad informática, soporte en sitio.

Anexo 8. Hardening propuesto para las instalaciones (Data Center)

## Implementaciones de seguridad físicas para el cuarto de equipos

### Objetivo

Definir lineamiento de seguridad a cumplir durante la ejecución de medidas preventivas para reducir el riesgo en el cuarto de equipos.

### Alcance

Es procedimiento aplica al cuarto de equipos para mejorar la seguridad mediante criterios definidos.

### Responsables – Participantes

Administrativo
Administrador de red
Seguridad informática

1. **Procedimiento general**

1.1. Evitar pasar los cables paralelos a los cables de corriente (mucho menos en el mismo caño).

1.2. No doblar los cables en un radio menor de menos de 4 veces su diámetro.

1.3. Si se agrupan los cables con sujeta cables, no apretarlos demasiado. Se pueden poner firmemente pero si se aprietan mucho, se pueden deformar los cables.

1.4. Mantener los cables lejos de dispositivos o electrodomésticos que puedan introducir "ruido" en ellos.

Una pequeña lista de aparatos prohibidos: fotocopiadoras, calentadores eléctricos, parlantes, impresoras, televisiones, luces fosforescentes, copiadoras, maquinas soldadoras, hornos microondas, teléfonos, ventiladores,

motores de elevadores, hornos eléctricos, secadores, lavadoras.

1.5. Evitar estirar los cables.

1.6. No pasar cables UTP por el exterior de las edificaciones. NUNCA, ya que al estar conectados atraen por ejemplo los rayos. Además Los cables que se usan para exteriores no son los mismos que los normales.

1.7. No usar clavos (grapas) para asegurar los cables a la pared. Usar ganchos para cable de teléfono o televisión como los que usa la compañía de cable cuando instala la antena. (Lenox)

Anexo 9. Técnicas, herramientas y análisis de la situación actual del Service Desk

| Aspectos a analizar | Marco de referencia | Técnica | Instrumentos / Herramienta informática | Codificación | Descripción |
|---|---|---|---|---|---|
| **RED, EQUIPOS** | ISO 27002<br>Informàtica Forense | **Software que permita identificar vulnerabilidades** | Nessus<br>Nmap<br>Conan (Inteco Cert) | **SW001**<br>**SW002**<br>**SW003** | **SW001:** Nessus: Permite identificar vulnerabilidades en la red.<br>**SW002:** Nmap: Permite explorar la red y realizar auditorías de seguridad.<br>**SW003:** Conan (Inteco Cert): Sistema de detección de vulnerabilidades del sistema operativo. (Belloso Ramiro, 2008) |
| | | **Entrevista** | Cuestionario | **ENTC001** | **ENT001:** Permite identificar los controles de seguridad existentes de la red interna del Service Desk (dirigido al administrador de la red)<br>**Fuente: ISO/IEC 27002 - 10,6**: Gestión de la seguridad de las redes |
| | | **Check List** | Check List | **CHL001** | **CHL001:** Verificar los controles existentes de red, y la seguridad de los servicios de la red (dirigido al administrador de la red)<br>**Fuente: ISO/IEC 27002 - 10,6:** Gestión de la seguridad de las redes |

| Descripción del trabajo realizado | Observaciones |
|---|---|
| SW001 - Nessus: Se tomó como muestra las IP's del grupo ACD (Call Tacker), y se realiza el análisis con la herramienta Nessus para la identificación de vulnerabilidades en la red y equipos seleccionados, de esta validación se detectó algunas novedades como equipos con permisos de administrador, puertos abiertos en la red, documentos sin clasificar.<br><br>Para continuar y realizar un mejor análisis se hace uso de dos herramientas adicionales NMAP y CONAN, estas herramientas fueron útiles para escaneo de IP's y análisis de servidores de archivos, cada herramienta fue corrida sobre la muestra tomada en principio que es el área de ACD del Service Desk, luego del trabajo realizado en la muestra se detectan vulnerabilidades como:<br><br>• Puertos abiertos<br>• Equipos con permiso de administrador<br>• Desbordamiento de Bufer<br>• Desactualización de navegador<br>• Antivirus desactualizado<br>• Actualizaciones pendientes de instalar<br>• Documentos sin clasificar | • Puertos abiertos<br>• Equipos con permiso de administrador<br>• Desbordamiento de Bufer<br>• Desactualización de navegador<br>• Antivirus desactualizado<br>• Actualizaciones pendientes de instalar<br>• Documentos sin clasificar |
| En entrevista mantenida con Nelly Suntaxi administradora de la red, se pudo conocer que la parte de infraestructura de la red interna de TCS del servicio Service Desk de Telefónica es monitoreada por Bradco empresa proveedora del servicio de monitoreo de las redes internas de TCS, esta empresa es conocida como Te uno, por lo que procedimientos de monitoreo , herramientas y alarmas son responsabilidad de ellos, Nelly como administradora lo que hace es entregarles las definiciones técnicas las mismas que Te uno configura en los equipos.<br><br>Te uno como empresa entrega a TCS un informe mensual de cómo se encuentran las configuraciones y el monitoreo que se realiza, en caso de que exista un inconveniente la alarma se les presenta a Te uno y es reportada al administrador de la red para conocimiento y toma de decisiones pero las configuraciones en caso de cambios la realizan ellos.<br><br>Por otro lado la parte de seguridad y certificación de la red interna del proyecto la realizo en su momento Seguridad Informática, Nelly no tiene conocimiento mayor de las seguridades y responsables de las mismas, por lo que como revisión se solicitará una entrevista al área de Seguridad Informática para la revisión de estos puntos.<br><br>La redundancia que se ha aplicado en la red es manual ya que no se cuenta con nada automático implementado en red, los dos enlaces de redundancia que existen para con el cliente Telefónica, también son manuales ya que se puede enviar la conexión a cualquiera de los enlaces pero es Telefónica quien debe autorizar el paso de información por el enlace elegido.<br><br>En entrevista mantenida con el personal de Seguridad informática conocemos que existen unos documentos internos de TCS conocidos como Hardening, estos contienen procedimientos y normativas a cumplir para la implementación de una red interna, se valida además que el proyecto Service Desk no cuenta con la certificación cuando se puso en producción, ni se realiza análisis de vulnerabilidades ya que este proceso de análisis no ha sido solicitado por las jefaturas a cargo del proyecto.<br><br>Los procedimientos existentes para las tareas como toma de control son internos de TCS ya que telefónica no ha impuesto ningún tipo de control ni ha solicitado de manera oficial el cumplimiento de ningún requerimiento de seguridad. | • Redundancia en la red manual<br>• Desconocimiento de procedimientos para el manejo y monitoreo de la red<br>• No existe análisis de vulnerabilidades<br>• No existe documentación del cliente para la seguridad en el servicio<br>• No existe documentación independiente del servicio<br>• Seguridades impuestas a la red básicas |
| El Check List se ha llenado con la ayuda de Arquitectura como administradores de la red y Seguridad Informática TCS, de este Check List podemos identificar que la red no ha sido certificada y no cuenta con todas las seguridades, que se mantiene un monitoreo y gestión manejada por el proveedor Te uno, también se puede verificar que no existen logs que permitan realizar un chequeo de configuraciones o cambios realizados más que solo de Firewall, las demás configuraciones en los equipos no son históricas, estos datos obtenidos entrarán a revisión y análisis para determinar observaciones o incumplimientos a lo normado por las buenas prácticas. | *logs de configuración de equipos no histórico<br>*Proyecto en producción no certificado<br>*excepciones a procedimientos sin conocimiento de Seguridad Informática |

| | | | | | |
|---|---|---|---|---|---|
| **INSTALACIONES** | ISO 27002 Informática Forense | **Check List** | Check List/EncuestaTick | **CHL002** | **CHL002**: Permite identificar si el Service Desk mantiene áreas seguras y los equipos se encuentran seguros. (dirigido al personal y observación directa) **Fuente: ISO/IEC 27002 - 9:** seguridad física y del entorno. |

| | |
|---|---|
| Según el Check List realizado mediante la herramienta informática EncuestaTick al personal del Service Desk se pudo evidenciar que se tiene varias brechas e incumplimientos en función al análisis de los resultados, es decir se tiene varias debilidades que deberían ser analizados por la alta gerencia y tomar planes de acción para que estos puedan ser mitigados o corregidos.<br><br>Se ha tomado un Check List de instalaciones de cuarto de equipos normado por la ISO para la validación, se realiza la visita en campo el 5 de Enero donde se puede observar el esta del cuarto de equipos, dentro de las oficinas del Edificio Pucará donde se encuentra el Service Desk también se encuentran más proyectos que dan servicio al cliente Telefónica, en una de las oficinas se ha designado un espacio para los equipos es espacio visible para todo el personal de esa área, no tiene seguridad para la revisión y no se encuentra aislado, no cuenta con ventilación independiente, no se tiene redundancia en la parte eléctrica ya que cuentan con UPS pero no se tiene topología para redundancia.<br><br>Se valida que la red ya se encuentra compartida para los demás proyectos también, parcialmente se tiene etiquetado y ordenados de los cables y equipos que se encuentran en el cuarto de equipos, se cuenta con cielo falso por donde se distribuye todo el cableado de los diferentes proyectos que ahí funcionan incluyendo el Service Desk, con respecto a seguridades físicas no se identifica que se cuente con seguridades, al ingreso lo que se realiza es un registro del ingreso de personal externo a los proyectos. Extintores y señalización están ubicados al rededor de todo el piso y el personal se encuentra capacitado en caso de emergencia, generadores adicionales de energía cuentan con el que el edificio ofrece por lo que conexión a tierra y pararrayos también está en manos de la administración del edificio. Las oficinas son cuartos amplios donde se encuentran distribuidos los ingenieros de soporte según su área, los cables de red que llegan a las estaciones de trabajo se encuentran visibles y sin orden. | • No se cuenta con redundancia de energía eléctrica<br><br>• No se mantiene una seguridad a los equipos<br><br>• No se tiene identificado el cableado por etiquetados correctos<br><br>• No existe orden en la distribución de la red<br><br>• No se tiene un proceso continuo de mantenimiento de equipos |

| | | | | | |
|---|---|---|---|---|---|
| **PROCEDIMIENTOS** | COBIT<br>ISO 27002 | **Entrevista** | Cuestionario | **ENT002** | **ENT002**: Permite conocer los procedimientos establecidos en la organización<br>(dirigido al PL del Service Desk)<br>**Fuente:** Cobit 4,1 |
| | | **Check List** | Check List/EncuestaTick | **CHL003** | **CHL003:** Permite identificar el grado de madurez de conocimiento de los procedimientos de seguridad<br>(dirigido al personal del Service Desk)<br>**Fuente:** ISO/IEC 27002 - 15: Cumplimiento<br>Cobit 4,1 |

| | |
|---|---|
| Según entrevista mantenida con líder del área de ACD del proyecto Service Desk Telefónica, indica que los procedimientos de manejo de información no se encuentran difundidos a nivel general en el personal, son de conocimiento de los líderes de área y líderes de proyecto esta información se encuentra disponible en el home folder, que es un repositorio de TCS al cual se tiene acceso por IP y en donde se encuentra disponible información considerada como confidencial, como contratos de TCS y procedimientos internos.<br><br>Telefónica como cliente no ha entregado documentación para el manejo o clasificación de la información por parte del proveedor lo que cuenta es con una clausula en el contrato firmado en el que se solicita confidencialidad de la información, por su parte Telefónica no realiza ningún tipo de seguimiento al cumplimiento a esta cláusula ni supervisa de alguna manera el manejo de información importante.<br><br>El área de soporte en sitio si cuenta con procedimientos entregados por el responsable del área en Telefónica, en estos procedimientos se describe el trato que se debe dar a un equipo y su información dependiendo del tipo de usuario al que pertenece, en este procedimiento se define también el tipo de preparación que se debe dar a un equipo antes de ser entregado a su custodio.<br><br>Procedimientos de seguridad, desarrollo o protección de la información han sido definidos de manera verbal no se tiene definido ningún tipo de documento para esto ya que todo se ha ido transmitiendo con personal que conoce del servicio y no existe documentación de los procedimientos a cumplir, lo que si se mantiene documentado son manuales de servicio en cada área. | • No se cuenta con procedimientos entregados por el cliente.<br>• No se poseen documentación alineada al cumplimiento del servicio.<br>• La información existente no ha sido difundida entre todo el personal.<br>• No existe una clasificación de información difundida ni aplicable a la documentación existente.<br>• No se encuentra difundido estrictamente los procedimientos de seguridad de información. |
| El Check List fue subido al internet y el link fue enviado al personal del Service Desk con el objetivo de identificar el grado de madurez del servicio según los procedimientos y conocimiento de los mismos dentro del personal, se obtiene 30 respuestas al Check List, las mismas han sido analizadas y por lo indicado por el personal se puede concluir que el servicio se encuentra en un nivel 2 según la matriz de madurez de COBIT que indica "se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto los errores son muy probables", esta calificación se le otorga ya que en el 70% de las encuestas el personal indica que la documentación existe pero no ha sido difundida en el personal, pero la documentación existente no está formalizada por la gerencia es documentación de apoyo al servicio, no cuenta con las autorizaciones y difusión necesaria. | • No se tiene un estándar en la documentación<br>• No se difunde los nuevos procedimientos al cliente<br>• Los procedimientos deberían basarse a la necesidad del cliente |

| | | | | | |
|---|---|---|---|---|---|
| **PERSONAL** | ITIL<br>COBIT | **Encuesta** | Cuestionario/EncuestaTick | **ENC001** | **ENC001:** Permite conocer el cumplimiento de los empleados en función a la seguridad de la Información (dirigido al personal del Service Desk)<br>Fuente: ITIL V3, COBIT 4,1 |
| | | **Observación directa** | Tarjeta de observación | **TOB001** | **TOB001:** Permite tener una lista de chequeo que sirve para registrar todo acto o condición insegura, con el fin de detectarlas, corregirlas y / o controlarlas y prevenir así la ocurrencia de incidentes o vulnerabilidades |

| | |
|---|---|
| En la encuesta realizada al personal interno del Service Desk vía internet se identifica algunas novedades en la seguridad y procesos internos, un gran porcentaje del personal no tiene conciencia de la importancia de la Seguridad de la Información, no se ha inculcado un interés por cumplir con las políticas de seguridad básicas en el servicio, las políticas de seguridad por la forma en cómo se tomó el servicio no han sido dadas a conocer al personal en su mayoría, y muchos de ellos desconocen la existencia de la documentación.<br><br>Se valida también que no se cuenta con un plan de mantenimiento continuo de los equipos para detección de inconvenientes o resolución de problemas existentes en los equipos, los equipos están siendo revisados el momento que se presenta un problema haciendo que esto afecte a la operatividad del servicio, tampoco se ha definido respaldos es decir no se cuenta con un plan de obtención de Backups, ocasionando que en caso de daños no se tenga respaldos de la información.<br><br>Se valida que no todos los equipos cuentan con la restricción de instalación de software es decir los usuarios están teniendo permisos de administrador en los equipos permitiéndoles instalar software sin control, se valida que tampoco el bloqueo de puertos USB ha sido efectivo en todos los equipos , con estos puntos el servicio no cuenta con seguridad de confidencialidad ya que al tener libre uso de USB la información puede ser transportada en medios magnéticos sin el consentimiento del cliente Telefónica. | • Instalan software externo<br>• Uso de dispositivos externos<br>• No se tiene un proceso de Backups continuo<br>• No todas las políticas de seguridad de información conoce el personal<br>• No se tiene un plan de mantenimiento de equipos<br>• Comparten contraseñas con el personal<br>• Usan papeles para divulgar contraseñas |
| Se valida con el personal de las 3 áreas del Service Desk el conocimiento y cumplimiento de los procesos existentes, para lo cual se ha realizado una visita a las instalaciones y se valida que cada área cuenta con procedimientos internos pero estos no están formalizados es decir no cuentan con la aprobación de la gerencia, en el caso de los procedimientos que maneja el área de aplicaciones han sido entregados por el cliente y están aprobados y autorizados para su uso, los procedimientos internos no han sido formalizados.<br><br>Se valida con el personal de las 3 áreas del Service Desk el conocimiento y cumplimiento de los procesos existentes, para lo cual se ha realizado una visita a las instalaciones y se valida que cada área cuenta con procedimientos internos pero estos no están formalizados es decir no cuentan con la aprobación de la gerencia, en el caso de los procedimientos que maneja el área de aplicaciones han sido entregados por el cliente y están aprobados y autorizados para su uso, los procedimientos internos no han sido formalizados.<br><br>Los colaboradores no conocen en su totalidad los procedimientos que existen a nivel de empresa y cliente. | • Procedimientos no formalizados<br>• Desconocimiento de procedimientos existentes<br>• Falta de difusión de procedimientos |

Anexo 10. Resultados obtenidos del análisis en el Service Desk

| | | |
|---|---|---|
| **VALIDACIÓN DE LA RED INTERNA DEL SERVICIO SERVICE DESK TELEFÓNICA - TCS**<br><br>**ISO 27002** | * Falta de controles de Seguridad de la información | En el marco de referencia ISO27002 en la parte de gestión de red (10.6.1 Controles de las redes literal c) se indica: "*Es conveniente establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas; también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados".*<br><br>Durante nuestras revisiones se verifica que la disponibilidad del servicio depende del enlace con el cliente, este enlace es redundante pero el cambio de enlace de conectividad es manual, ya que se depende del administrador a cargo para la activación de paso de información por el enlace seleccionado.<br><br>Adicional a esto el servicio en las estaciones de trabajo y red en general tiene algunas vulnerabilidades claras como:<br>* Se identificaron Puertos de conexión abiertos<br>* Equipos de ingenieros de soporte con permiso de administrador<br>*Desbordamiento de Búfer<br>*Estaciones de trabajo con navegadores desactualizados<br>*Antivirus desactualizado<br>*Actualizaciones pendientes de instalar<br>*Documentos sin clasificar |
| | * Desde el inicio del proyecto hasta la fecha no se ha realizado un análisis de vulnerabilidades. | En el estándar de seguridad ISO27002 en su parte de gestión de red (10.6.1 Controles de las redes literal e) indica: "*se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información*.", sin embargo se validado y no existe evidencia de un análisis de vulnerabilidades al servicio, se valida que los controles que se han aplicado son el resultado de inconvenientes que se han presentado y no como medidas preventivas. |
| | * Telefónica no ha entregado documentación con respecto a la seguridad de la información que se debe tener en el servicio.<br><br>* TCS no cuenta con documentación con respecto a la seguridad de información que se debe tener en el servicio con Telefónica. | En el estándar de seguridad ISO27002 en la parte de seguridad de los servicios de red (10.6.2 Seguridad de los servicios de la red literal c) indica: "*Procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red o a las aplicaciones, cuando sea necesario.*".<br><br>En entrevista con los supervisores y líder proyecto del Service Desk, se puede identificar que el cliente Telefónica no ha emitido ningún procedimiento formal para la utilización de la red y enlaces, TCS por su parte tampoco ha definido documentación para el uso de la red del proyecto Service Desk Telefónica - TCS, TCS con lo que cuenta es con documentación que permite la configuración, que son los manuales conocidos como Hardenings, basados en buenas prácticas de seguridad en redes. |

| | | |
|---|---|---|
| | * Las seguridades aplicadas a la red interna son básicas, solo cumplen con parte del Hardening de seguridad.<br><br>*Todo proyecto puesto en producción debe constar con la certificación de seguridad el Service Desk, no ha sido certificado.<br><br>*Dentro de la red del Service Desk se ha incluido más proyectos por lo que se han realizado excepciones a procedimientos sin conocimiento de Seguridad Informática. | En el estándar de seguridad ISO27002 dentro de la descripción de gestión de red (10.6.1 Controles de las redes ) indica: "*Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado." además recomienda "se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.*".<br><br>Durante la revisión y análisis realizado con respecto a la red se valida que la seguridad del proyecto no fue certificada desde sus inicios, y que lo único que valido su puesta en producción fue el cumplimiento de algunos puntos del Hardening de redes de TCS, además se pudo observar que los cambios e inclusiones que se han realizado en la red no ha sido notificada a Seguridad Informática TCS y no cuentan con su autorización por lo que existe excepciones en las configuraciones que no han sido aprobadas.. |
| | * A nivel de administración de la red se desconoce procedimientos para la configuración y monitoreo de la red. | En el estándar de seguridad ISO27002 dentro de la descripción de gestión de red ((10.6.1 Controles de las redes literal d) indica: "*se deberían aplicar el registro y el monitoreo adecuados para permitir el registro de acciones de seguridad pertinentes;*".<br><br>TCS ha contratado a Te uno para la configuración y monitoreo de sus enlaces y redes de los diferente proyectos, en entrevista con la administradora de la red se puede identificar desconocimiento en los procedimientos que Te uno utiliza para dar el servicio, lo que se está realizando es emitir el requerimiento sin validar la forma de configuración, así mismo con el monitoreo no conocen el tipo de herramienta que utilizan ni qué tipo de alarmas emiten el momento de que se detecta una falla en el enlace. |
| | *El registro de acciones se mantiene en logs de configuración de equipos, que cuando se configuran nuevamente se borra el anterior por lo que hay logs históricos. | En el estándar de seguridad ISO27002 dentro de la descripción de gestión de red ((10.6.1 Controles de las redes literal d) indica: *"se deberían aplicar el registro y el monitoreo adecuados para permitir el registro de acciones de seguridad pertinentes;".*<br><br>En la entrevista mantenida con la administradora a cargo de la red del proyecto Service Desk Telefónica - TCS, podemos identificar que se cuenta con logs de acciones en la configuración de equipos y firewalls, sin embargo estos logs no son almacenados en ningún repositorio histórico, solo el log de firewall está siendo almacenado de manera histórica. |

| RIESGO | ANÁLISIS | MEDIDA PREVENTIVA |
|---|---|---|
| En caso de tener que hacer uso de la conexión al otro enlace depende de la disponibilidad del administrador a cargo, por parte del cliente, haciendo que se pierda la continuidad del servicio.<br><br>Se debe salvaguardar la información y con las vulnerabilidades presentadas se tiene el riesgo de que la información que el servicio maneja sea ultrajada o que debido a ataques constantes se pierda información y esta sea difundida maliciosamente, haciendo que sobre el proveedor TCS caigan multas económicas y hasta demandas por incumplimientos. | No se ha trabajado conjuntamente con Seguridad informática para mejorar y establecer controles en la red interna, en este momento solo se encuentra puesto en operación el Hardening interno de TCS, para nuestra revisión se ha utilizada herramientas de investigación de informática forense, según lo encontrado por las herramientas indica que se tiene:<br>• Se identificaron Puertos de conexión abiertos<br>• Equipos de ingenieros de soporte con permiso de administrador<br>• Desbordamiento de Búfer<br>• Estaciones de trabajo con navegadores desactualizados<br>• Antivirus desactualizado<br>• Actualizaciones pendientes de instalar<br>• Documentos sin clasificar<br>Con lo cual la red está propensa ataques internos. Adicional se ha identificado que no se ha realizado un análisis de vulnerabilidades a la red interna desde su puesta en producción, ni se ha realizado actualizaciones o tomado respaldos de información, esto se ha dado debido a que los proyectos han salido a producción en tiempos record sin mayor revisión.<br>Los errores y criterios negativos encontrados no pueden ser considerados como riesgo crítico sino más bien riesgo moderado debido a que el proyecto es pequeño sin embargo se debe tomar los correctivos necesarios para evitar pérdidas de continuidad en el servicio que terminarían en sanciones por parte del cliente. | Realizar un análisis de errores ya presentados encontrando la causa por la que se han presentado y aplicar medidas de seguridad en la red interna del servicio. |
| Sin realizar análisis de vulnerabilidades periódicos, se tiene una red insegura, lo cual puede ocasionar que se tengan ataques a la red, haciendo que se pierda la continuidad del servicio. | | Realizar una revisión a los procesos de monitoreo y administración que aplica TEUNO en el servicio que oferta a TCS y acordar la elaboración de una bitácora de logs o un histórico de configuración con el fin de mitigar inconvenientes de manera rápida y eficaz. |
| TCS en desconocimiento de procedimientos internos del cliente Telefónica para el uso de red y enlaces podría estar incumpliendo normas que podrían incurrir en problemas legales o multas económicas al servicio. | | Mantener reuniones periódicas con el cliente con el fin de mejorar la calidad del servicio y emitir planes de acción para el correcto manejo de la información del cliente. |

| | | |
|---|---|---|
| La certificación de seguridad en la red de alguna manera indica que la red no es propensa a ataques ni caídas, por lo comentado, al no contar con las autorizaciones de seguridad y solo realizar las configuraciones a nivel de Infraestructura es decir de administración de la red no se garantiza funcionalidad optima, ya que puede sufrir caídas o ataques maliciosos ocasionando perdida de continuidad del servicio. | | Trabajar conjuntamente con seguridad informática para mantener la certificación de seguridad de red en el Service Desk, así mejorará la calidad y seguridad en la trasmisión de datos cliente - proveedor.<br><br>Realizar una Vlan independiente del Service Desk para mejorar la administración y seguridad de la red. |
| TCS al ser dueño de los enlaces que Te uno monitorea y configura debe conocer qué tipo de procedimientos se están cumpliendo para dar el servicio, el no conocer sobre los procedimientos y forma de monitoreo puede ocasionar que no se estén reportando inconvenientes en los enlaces, ya que para el proveedor pueden resultar insignificantes. | | Realizar capacitaciones con el proveedor TE UNO con el fin de conocer la administración de la red y el monitoreo. |
| Al no contar con logs históricos de las configuraciones y acciones que se realizan en los switch y routers. La configuración original autorizada por seguridad informática TCS y revisada por Telefónica puede ser alterada drásticamente, facilitando ataques a la red interna. | | Mantener una bitácora de logs o un histórico con el fin de realizar monitoreos continuos y mitigar las vulnerabilidades que se puedan presentar en la operación del servicio. |

**INSTALACIONES**

| | | |
|---|---|---|
| **VALIDACIÓN DE LAS INSTALACIONES DEL CUARTO DE SERVICIOS DEL PROYECTO SERVICE DESK TELEFÓNICA - TCS**<br><br>**ISO 27002** | *Para el ingreso y acceso al cuarto de equipos no se mantiene un proceso de seguridad implementado. | El estándar de seguridad en su definición de Seguridad Física y del Entorno (9.1 ÁREAS SEGURAS) indica que: *"Los servicios de procesamiento de información sensible o crítica deberían estar ubicados en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia."*<br><br>De la revisión realizada se puede identificar que el acceso al cuarto de equipos es libre ya que se encuentra dentro de una de las oficinas del primer piso del edificio Pucara, en un espacio definido en una de las oficinas, y no existe un control o procedimiento de Seguridad que controle el acceso no autorizado al cuarto de equipos. |
| | *No se cuenta con redundancia de energía eléctrica. | El estándar de Seguridad ISO27002 en su descripción de continuidad del negocio (14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio literal e) indica que: *"identificación y consideración de la implementación de controles preventivos y mitigantes adicionales;"*, sin embargo al revisar las instalaciones se valida que los controles preventivos con respecto a la energía eléctrica no se ha tomado en cuenta la redundancia, es decir si la única fuente sufre algún daño no se tiene otra fuente de energía. |
| | * Desorden en el cuarto de equipos. | El estándar de Seguridad ISO27002 en su descripción de continuidad del negocio ( (14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio literal j)) indica que: *"garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización;".*<br><br>De la revisión realizada el cuarto de equipos tiene falencias dentro de ellas:<br><br>*No se tiene identificado el cableado por etiquetados correctos.<br>*No existe orden en la distribución de la red. |

| RIESGO | ANÁLISIS | MEDIDA PREVENTIVA |
|---|---|---|
| Al no contar con un control de acceso ni seguridades en el ingreso al cuarto de equipo se corre el riesgo de intencional o no, se realicen cambios en el cableado de los equipos ahí existentes o desconexión de los mismos. | Para la revisión de las instalaciones correspondientes al cuarto de equipos del proyecto Service Desk Telefónica - TCS, se utilizó uno de los marcos de referencia escogidos la ISO 27002, la toma de información y captura de evidencias se apoyó en las herramientas de entrevistas, Check List y observación directa. De la revisión realizada al cuarto de equipos bajo estas características se ha identificado 3 criterios que podrían llegar a ser un problema o que en su momento provocaron una perdida en la continuidad del servicio.<br><br>Dentro del marco de referencia escogido para las instalaciones podemos interpretar de su teoría lo siguiente: | Aplicar control de acceso al cuarto de equipos a más de la bitácora manual, estudiar la factibilidad de aislar el cuarto de quipos y colocar seguridad al ingreso al mismo. |
| El servicio ofertado es 24 X 7 por lo que se ha tenido inconvenientes de fallas con la fuente de energía eléctrica en horas de la noche y no se ha podido solventar por falta de otra fuente de energía, cuando es una desconexión se activa la planta de energía eléctrica pero si es problema de fuente se suspende el servicio hasta su corrección. | Toda instalación en la que se encuentre equipos de comunicación o encargados de la transmisión de información debe contar con seguridades físicas establecidas, controles de acceso, redundancia en el funcionamiento para evitar pérdidas de continuidad, y un orden en la distribución de cables, para todo lo normado dentro de un marco de referencia se tiene conocidas buenas practicas que permiten cumplir con las seguridades, orden y redundancia que es lo más fuerte con lo que debería contar un cuarto de equipos, claro que cada uno de estos puntos debe ser analizado para el tamaño de cuarto de equipos y por el servicio que oferta y la funcionalidad que cumple. | Realizar un análisis conjuntamente con gerencia para conocer la factibilidad de la implementación de redundancia de energía eléctrica. |
| El desorden dentro del cuarto de equipos puede ocasionar confusión en la distribución de los recursos de la red, a más de que el trabajar sin etiquetados y distribución no identificada complica los mantenimientos. | | Implementar las mejores prácticas para realizar el levantamiento y organización en el cuarto de equipos con el fin de mejorar la calidad y la gestión de los equipos. |

## PROCEDIMIENTOS

| | | |
|---|---|---|
| **REVISIÓN PROCEDIMIENTOS EXISTENTES EN PROYECTO SERVICE DESK TELEFÓNICA - TCS**<br><br>**COBIT 4.1** | *No existe documentación alineada al cumplimiento del servicio y objetivos de TI. | COBIT en el Dominio de Planificación y Organización en el objetivo de control P02. Definir la Arquitectura de la Información. Indica que: *"La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad."*<br><br>De las revisiones realizadas a los procedimientos existentes, TCS cuenta con documentación pero a nivel general no se ha elaborado procedimientos orientados al tipo de servicio que se le brinda a Telefónica, los procedimientos existentes están más orientados al servicio que se entrega como empresa a entidades financieras. |
| | *La información existente no ha sido difundida entre todo el personal. | COBIT en el Dominio de Planificación y Organización en el objetivo de control PO6.4 Implantación de Políticas de TI indica que debe: *"Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales."*<br><br>De las revisiones realizadas con respecto al conocimiento de información existente en el proyecto tanto por parte de TCS como de Telefónica, identificamos que existe documentación que ayudaría a normar el servicio pero no esta no ha sido difundida entre el personal ya que no hay conocimiento de su existencia entre los colaboradores. |
| | *No existe una clasificación de información difundida ni aplicable a la documentación existente.<br>* No se cuenta con procedimientos entregados por el cliente. | COBIT en el Dominio de Planificación y Organización en el objetivo de control PO2.3 Esquema de Clasificación de Datos indica que se debe: *"Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado."*<br><br>Al realizar la revisión de la documentación existente y los procedimientos que al momento se cumplen identificamos que no se ha definido una clasificación de información que de alguna manera se pueda identificar y dar el trato correspondiente. |

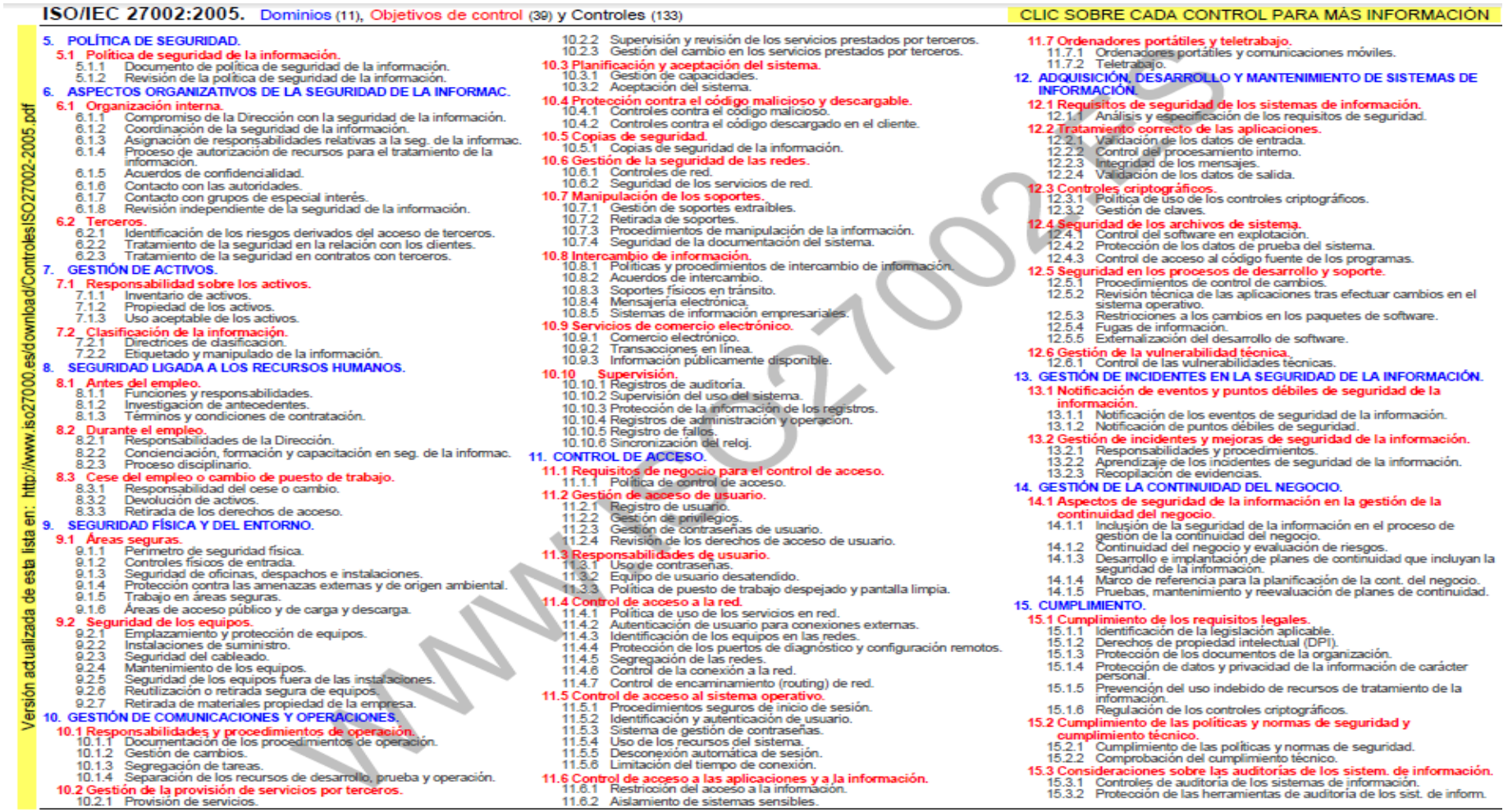
| RIESGO | ANÁLISIS | MEDIDA PREVENTIVA |
|---|---|---|
| TCS en su gama de documentos no ha definido procedimientos para el tipo de servicio lo cual estaría dejando a libertad del líder de proyecto la forma de cumplir el servicio, teniendo falencias ocasionando inconformidad con el servicio y mala imagen de la empresa. | Para la revisión de los procedimientos nos apoyamos en herramientas de investigación como Entrevistas, Check List teniendo el siguiente análisis. De la revisión se puede ver que la poca documentación que existe del proveedor no se encuentra alineada al Servicio ya que la mayoría de información está orientada a los servicios que más abarca TCS que son los servicios a entidades bancarias. Perjudicando a la entrega de servicio a entidades como Telefónica que nada tienen que ver con la Banca. El Service Desk cuenta con documentación para la entrega del servicio según el área pero esta documentación se encuentra disponible en un compartido pero al personal sobre todo al personal nuevo no se le ha indicado que contiene cada documento. La falta de distribución de información y documentación puede provocar fallas en el cumplimiento de niveles al ser un proyecto con alto grado de rotación de personal debería mantener todo el tiempo un plan de difusión o comunicación de la existencia de la documentación que aunque no está aprobada por la gerencia es de gran apoyo en la entrega del Servicio. De las revisiones realizadas podemos identificar que no se ha realizado una clasificación de información, es decir el personal que manipula la información desconoce si la información con la que está trabajando es confidencial, sensible, pública o si tiene algún grado de criticidad. | Revisar la documentación existente y actualizarla de ser el caso para el tipo de servicio que se oferta con Telefónica. |
| Al no ser difundida la información en el personal, se tienen incumplimientos a lo normado y esto podría incurrir en faltas al servicio, ocasionando multas a TCS o sanciones mayores al personal. | | Realizar un plan de acción para difundir los procedimientos a todo el personal del Service Desk con el fin de que el equipo conozca, y sobre todo aplique en la gestión diaria. |
| Si la información no cuenta con clasificación normada, puede ser tratada sin importancia poniendo a disposición información confidencial, esta clasificación no ha sido definida ni por el cliente ni por la empresa encargada de dar el servicio. | | Implementar un procedimiento para la clasificación de la información, mediante varios niveles de severidad (crítica, media, baja) mediante un formato común. |

**PERSONAL**

| | | |
|---|---|---|
| **REVISIÓN PERSONAL DEL PROYECTO SERVICE DESK TELEFÓNICA – TCS**<br><br>**ITIL V3** | *Procedimientos de servicio no formalizados. | ITIL la definición teórica de ITIL V3 indica: *"El desarrollo más significativo ha sido el paso de un marco de trabajo basado en procesos a una estructura integral que refleje el ciclo de vida de los servicios de TI."*<br><br>Las 3 áreas del Service Desk cuentan con documentación de procedimientos que cumplen para dar el servicio pero las mismas no tienen ninguna formalidad para ser difundidas, por lo que el personal no estaría obligado a utilizarlas. |
| | *Desconocimiento de procedimientos de servicio existentes. | ITIL en su contexto del Diseño del Servicio (SD) en Gestión de la capacidad del servicio indica: *"La gestión de extremo a extremo, control y predicción del desempeño y la capacidad de servicios en vivo."*<br><br>Se valida con personal del Service Desk y se identifica que no se puede realizar esta gestión de extremo a extremo ya que el personal no conoce que existen manuales internos sin formalizar que detallan la forma de brindar el servicio según el área en la que se encuentre. |
| | *Falta de difusión de procedimientos. | ITIL en su contexto del Diseño del Servicio (SD) en Entregables de la gestión de la información y de la gestión de capacidad indica: *"Sistema de información de la gestión de capacidad: negocio, componentes de servicios y datos financieros; plan de capacidad; informes basados en los componentes; informes basados en servicios; informes de excepción; pronósticos y predicciones."*<br><br>De la revisión se valida que no existe un plan de difusión a nivel del Servicio lo conocido es que el supervisor de área reúna a su equipo y le comunique cambios en la documentación de procedimientos del servicio o del área o se notifique mediante correo a todo el personal, este es un procedimiento que lo han adoptado como buena práctica pero el mismo no está formalizado. |

| RIESGO | ANÁLISIS | MEDIDA PREVENTIVA |
|---|---|---|
| Los procesos existentes son documentación que permite dar el servicio pero no cuenta con la autorización de las jefaturas del proyecto para su uso por lo que el personal no está normado y el servicio no está siendo alineado ni normado. Esto ocasiona faltas al servicio e incumplimiento en los niveles. | De esta revisión se ha encontrado aspectos que el personal ha indicado no conocer o que se observa falencias en los procesos de servicio.<br>Este punto también fue analizado con la normativa de COBIT en su madurez de procedimientos y se lo vuelve a encontrar en la revisión realizada al personal mediante ITIL.<br>El no tener procedimientos formalizados puede ocasionar que si existe fallas las multas y errores sean responsabilidad del ingeniero de soporte<br>Como indicamos en el punto anterior los líderes de proyecto del Service Desk se han despreocupado en gran parte de conocer la documentación existente por lo que no han exigido su difusión en el personal y asumen que la capacitación ira pasando de operador en operador.<br>La falta de difusión en el personal es responsabilidad directa del personal a cargo de cada área que al igual que los líderes de proyecto asume el conocimiento de la documentación por parte de los ingenieros de soporte.<br>Durante nuestras revisiones se puede observar manuales no formalizados pero que contienen procedimientos a problemas existentes en el cliente que han sido corregidos y probados. Por lo que al no saber su existencia exige al ingeniero de soporte nuevamente consultar e investigar una solución a algo que ya está definido. | Implementar un proceso para la formalización de nuevos procedimientos ya sea de servicio, personal, seguridad u otros. El mismo deberá ser aprobado por gerencia para su respectiva calificación. |
| Si el personal desconoce procedimientos de servicio, el mismo está pasando de forma verbal con un gran alto nivel de error y la calidad del servicio entregado ira bajando cada vez más. | | Realizar una capacitación al personal en la que se recuerde o comunique los procedimientos contratados. |
| Si el personal desconoce procedimientos de servicio, el mismo está pasando de forma verbal con un gran alto nivel de error y la calidad del servicio entregado ira bajando cada vez más. | | Realizar un plan de acción para difundir los procedimientos a todo el personal, ya sea automática o manualmente |

Anexo 11. Norma ISO 27002



**ISO/IEC 27002:2005.** Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
- 5.1 Política de seguridad de la información.
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- 6.2 Terceros.
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- 7.1 Responsabilidad sobre los activos.
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- 7.2 Clasificación de la información.
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 8.1 Antes del empleo.
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- 8.2 Durante el empleo.
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- 8.3 Cese del empleo o cambio de puesto de trabajo.
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- 9.1 Áreas seguras.
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- 9.2 Seguridad de los equipos.
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- 10.1 Responsabilidades y procedimientos de operación.
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- 10.2 Gestión de la provisión de servicios por terceros.
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- 10.3 Planificación y aceptación del sistema.
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- 10.4 Protección contra el código malicioso y descargable.
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- 10.5 Copias de seguridad.
  - 10.5.1 Copias de seguridad de la información.
- 10.6 Gestión de la seguridad de las redes.
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- 10.7 Manipulación de los soportes.
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- 10.8 Intercambio de información.
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- 10.9 Servicios de comercio electrónico.
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- 10.10 Supervisión.
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- 11.1 Requisitos de negocio para el control de acceso.
  - 11.1.1 Política de control de acceso.
- 11.2 Gestión de acceso de usuario.
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- 11.3 Responsabilidades de usuario.
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- 11.4 Control de acceso a la red.
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- 11.5 Control de acceso al sistema operativo.
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- 11.6 Control de acceso a las aplicaciones y a la información.
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- 11.7 Ordenadores portátiles y teletrabajo.
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- 12.1 Requisitos de seguridad de los sistemas de información.
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- 12.2 Tratamiento correcto de las aplicaciones.
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- 12.3 Controles criptográficos.
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- 12.4 Seguridad de los archivos de sistema.
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- 12.5 Seguridad en los procesos de desarrollo y soporte.
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Control de las vulnerabilidades técnicas.

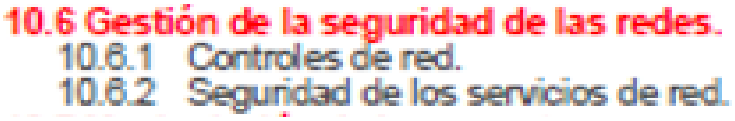
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 13.1 Notificación de eventos y puntos débiles de seguridad de la información.
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- 13.2 Gestión de incidentes y mejoras de seguridad de la información.
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
- 15.1 Cumplimiento de los requisitos legales.
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- 15.3 Consideraciones sobre las auditorías de los sistem. de información.
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

**Dominios, objetivos de control y controles utilizados**

**Red**




### 10.6.1. Controles de red

#### Guía de implementación

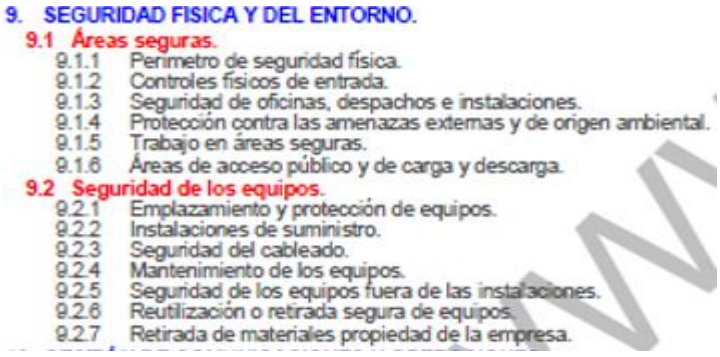
Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado.

### 10.6.2. Seguridad de los servicios de red

#### Información adicional

Los servicios de red incluyen la provisión de conexiones, servicios de red privada y redes con valor agregado, así como soluciones de seguridad de red administrada, como por ejemplo barreras de fuego *(Firewalls)* y sistemas de detección de intrusión. Estos servicios pueden ir desde simples anchos de banda no administrados hasta ofertas complejas de valor agregado.

**INSTALACIONES**




### 9.1.1. Perímetro de seguridad física

#### Control

Se deberían utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para

proteger las áreas que contienen información y servicios de procesamiento de información.

### 9.1.2. Controles físicos de entrada

**Control**

Las áreas seguras deberían estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

**Dominios utilizados de COBIT 4.1.**

| |
|---|
| COBIT en el Dominio de Planificación y Organización en el objetivo de control P02. Definir la Arquitectura de la Información. Indica que: *"La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad."* |
| COBIT en el Dominio de Planificación y Organización en el objetivo de control PO6.4 Implantación de Políticas de TI indica que debe: *"Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales."* |
| COBIT en el Dominio de Planificación y Organización en el objetivo de control PO2.3 Esquema de Clasificación de Datos indica que se debe: *"Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado."* |

**Recomendaciones utilizadas de ITIL V3**

| |
|---|
| ITIL la definición teórica de ITIL V3 indica: *"El desarrollo más significativo ha sido el paso de un marco de trabajo basado en procesos a una estructura integral que refleje el ciclo de vida de los servicios de TI."*<br><br>Las 3 áreas del Service Desk cuentan con documentación de procedimientos que cumplen para dar el servicio pero las mismas no tienen ninguna formalidad para ser difundidas, por lo que el personal no estaría obligado a utilizarlas. |
| ITIL en su contexto del Diseño del Servicio (SD) en Gestión de la capacidad del servicio indica*: "La gestión de extremo a extremo, control y predicción del desempeño y la capacidad de servicios en vivo."*<br><br>Se valida con personal del Service Desk y se identifica que no se puede realizar esta gestión de extremo a extremo ya que el personal no conoce que existen manuales internos sin formalizar que detallan la forma de brindar el servicio según el área en la que se encuentre. |
| ITIL en su contexto del Diseño del Servicio (SD) en Entregables de la gestión de la información y de la gestión de capacidad indica: *"Sistema de información de la gestión de capacidad: negocio, componentes de servicios y datos financieros; plan de capacidad; informes basados en los componentes; informes basados en servicios; informes de excepción; pronósticos y predicciones."*<br><br>De la revisión se valida que no existe un plan de difusión a nivel del Servicio lo conocido es que el supervisor de área reúna a su equipo y le comunique cambios en la documentación de procedimientos del servicio o del área o se notifique mediante correo a todo el personal, este es un procedimiento que lo han adoptado como buena práctica pero el mismo no está formalizado. |